Managing cyber-risk and security in the global supply chain: a systems analysis approach to risk, structure and behaviour

Sepúlveda Estay, Daniel Alberto

Publication date:
2017

Document Version
Publisher's PDF, also known as Version of record

Managing cyber-risk and security in the global supply chain: A systems analysis approach to risk, structure and behaviour

Daniel A. Sepulveda Estay

PhD Thesis

November 2017

Department of Management Engineering
Technical University of Denmark

Supervisor Professor Jesper Larsen, PhD.
Department of Management Engineering
Technical University of Denmark
2800 Kongens Lyngby, Denmark

Co-supervisor Professor Omera Q. Khan, PhD
Department of Business and Management
The Faculty of Engineering and Science
Aalborg University
2450 Copenhagen, Denmark

"A crisis is a terrible thing to waste" – Paul Romer

Preface

This PhD thesis is the product of the PhD project carried out by Daniel Alberto Sepulveda Estay at the Management Engineering department of the Technical University of Denmark. The project started on November 03rd, 2014 and ended on October 31st, 2017. This thesis is manuscript-based. However, the following are some of the Conference and Journal papers that were produced during the research (see Appendix 11.6).

Journal papers

P1 Khan, O., Sepúlveda Estay, D.A. 2015. *Supply Chain Cyber-Resilience: Creating an Agenda for Future Research*. Technology Innovation Management Review, no. April, pp. 6-12.

P2 Sepulveda Estay, D.A., Khan, O. 2017. *An endogenous exposure calculation method for cyber-risk assessment in supply chains*. Industrial Management & Data Systems Journal. *In review*

Conference papers

P3 Sepúlveda Estay, D.A., Khan, O. 2015. *Extending supply chain risk and resilience frameworks to manage cyber risk*. Paper presented at 22nd

EurOMA Conference, Neuchâtel, Switzerland, 26/06/2015 - 01/07/2015,

P4 Sepúlveda Estay, D.A., Khan, O. 2016. *Control Structures in supply chains as a way to manage unpredictable cyber-risks*. Paper presented at 5th World Production and Operations Management Conference, Havana, Cuba, 06/09/2016 - 10/09/2016,

P5 Sepúlveda Estay, D.A. & Khan, O. 2017. *A system dynamics case study of resilient response to IP theft from a cyber- attack*. Paper presented at 2017 International Conference on Industrial Engineering and Engineering Management (IEEM), Suntec City, Singapore, 10/12/2017 - 13/12/2017,

Dansk Resume

Truslen om cyber-angreb fortsætter med at vokse og forstyrre globale forsyningskæder. Denne trussel kan potentielt skade eller fuldstændig standse den daglige operation og dermed påvirke forretningens resultater og omdømme negativt. Derudover kan cyber-angreb potentielt resultere i langsigtede juridiske konsekvenser. Som følge heraf er der udgivet påfaldende lidt materiale om konsekvenserne af cyber-angreb. Virksomheders forsyningskæder fortsætter med at forberede sig på cyber-angreb gennem en blanding af traditionelle risiko- og resilience-frameworks for at beskytte deres netværk gennem patches, firewalls og antivirus eller gennem økonomiske forsikringer. Disse tilgange har dog ikke ført til de ønskede resultater, hvilket afspejles i den stadige stigning i forstyrrelser fra cyber-angreb.

Denne afhandling undersøger og foreslår værktøjer til styring af cyber-risici i forsyningskæden gennem en analyse, der følger tre overordnede trin. I trin 1 udføres et systematisk litteraturstudie for at analysere eksisterende viden om forsyningskæders cyber-resilience og identificere mangler i litteraturen. To væsentlige mangler i den eksisterende litteratur behandles i detaljer: 1) behovet for at forstå de særlige karakteristika for cyber-risici samt

hvordan disse karakteristika differentierer sig fra andre risici i forsyningskæden i forhold til effektiv risikostyring og 2) anvendelsen af systemtænkning til at behandle aspekter af silotænkning, statisk fokus og afhængigheden af historiske data til håndteringen af cyber-risici og cyber-resilience i forsyningskæden. I trin 2 undersøges førstnævnte mangel i litteraturen ved at identificere de særlige karakteristika ved cyber-risici ud fra rapporter om cyber-angreb. Slutteligt anvendes i trin 3 metoder fra systemtænkning i casestudier for at vurdere anvendeligheden af disse metoder i forhold til at adressere silo-tænkning, dynamik og historisk afhængighed for bedre at kunne håndtere cyber-risici og cyber-resilience.

Resultaterne af forskningen fordeler sig på tre hovedområder. For det første afslører undersøgelsen relevante mangler i de traditionelle metoder til styringen af cyber-risici, eksempelvis i forhold til at tage højde for dynamisk adfærd, utilstrækkelig eller vanskelig rapportering af hændelser, afhængigheden af historiske data til håndtering af ukendte eller nye angreb, samt en anvendt silo-tilgang til at håndtere et tværfagligt problem. For det andet identificeres relevante forskelle mellem cyber-risici og andre risici i forsyningskæden, som eksempelvis evnen til ikke at blive opdaget, den høje reproducerbarhed, evnen til at påvirke forskellige geografiske placeringer samtidig, og kompleksiteten af

cyber-angreb. Endelig afslører undersøgelsen at anvendelsen af metoder baseret på systemtænkning til at styre cyber-risici samtidig adresserer mangler i traditionelle metoder og giver grundlag for at tænke på cyber-risici som resultatet af ufuldstændige krav til design af forsyningskæder frem for at tænke på cyber-risici som en ydre trussel. Denne ændring i fokus giver forsyningskæder muligheden for at minimere tab ved at forberede systemet til at reagere på hvilken som helst cyber-risiko, der måtte føre til driftsforstyrrelser.

Resultaterne af denne forskning har både forskningsmæssige og praktiske implikationer. Ud fra et forretningsmæssigt perspektiv kan forsyningskæder drage fordel af at designe den adfærd, de har behov for gennem tværfaglige, simuleringsbaserede teknikker. Set fra et akademisk perspektiv vil forskere kunne drage fordel af 1) justering af rapporteringstider for at matche den hurtige udviklingscyklus for cyber-angreb, 2) konsolidering af et tværfagligt forskningsfællesskab inden for cyber-risiko og cyber-resilience, og 3) udvidelse af eksisterende forskningsmetoder ved at integrere dynamisk systemtænkning i dataindsamling og analyse.

Summary

The threat of cyber-attacks continues to grow and disrupt global supply chains, exposing companies to disruptions that severely affect or completely halt normal operations. This impacts business performance negatively through the company's bottom line and reputation, even resulting in long-term legal ramifications. As a result, little information about attacks and their consequences is published. Supply chains continue to prepare for cyber-attacks through a mix of traditional risk and resilience frameworks, protecting their networks through patches, firewalls and antiviruses, or financially through insurance. Yet these approaches are not giving the expected results, as reflected by the steady increase in disruptions from cyber-attacks.

This thesis investigates and proposes tools for managing cyber-risks in the supply chain, derived from an analysis that follows three main steps. In step one, existing knowledge about supply chain cyber-resilience is analysed through a systematic literature review, and gaps are identified. Two of the identified gaps are addressed in detail, 1) insufficient understanding of the particular characteristics cyber-risks and how these compare to other supply chain risks for effective risk management, and 2) insufficient

address by current methods to aspects of compartmentalization, static focus and history-dependence in the management of supply chain cyber-risk and cyber-resilience. Step two of this thesis explores the first gap by identifying the particular characteristics of cyber-risks from cyber-attack report data. Finally in step three methods based on systems thinking are applied to case studies to evaluate the degree to which these methods address compartmentalization, dynamics and history dependency in their application to the management of cyber-risk and cyber-resilience.

The findings of the research are in three main domains. First, the research reveals relevant gaps in the traditional methods available for the management of cyber risks, in areas such as their consideration of dynamic behaviour, inadequate or difficult reporting of events, their dependence on historical data to manage unknown or new attacks, and a silo-approach for managing a problem that is cross-disciplinary. Second, relevant differences between cyber-risks and other supply chain risks are identified, in areas such as the capacity of disruptions from cyber risks to go undetected, the high reproduction fidelity of cyber-risks, the capacity of cyber risks to affect different geographical locations simultaneously, and the complexity of cyber-attacks. Finally, the research reveals that the novel use of methods based in systems thinking for managing cyber-risks at the same time address gaps

found in traditional methods, and provide a foundation for thinking about cyber-risks not as an outside threat, but rather as the result of incomplete requirements to the supply chain design. This change in focus could allow supply chains to minimize losses by preparing the system for reaction to whatever cyber-risk leads to an operational disruption.

The findings of the research have both industrial implications. The industrial implications suggest supply chains can benefit from designing the behaviours they require through cross-disciplinary, simulation-based techniques. The academic implications suggest that researchers will benefit from 1) adjusting reporting times to match the quick development cycle of cyber-attacks, 2) consolidating a cross-disciplinary cyber-risk and resilience research community, and 3) expanding existing research methods by integrating dynamic systems thinking into data gathering and analysis

Acknowledgements

The process of completing my PhD project has come to an end. It has taken years of challenges and hard work, yet at the same it has been a time for insights and discovery. I am tremendously grateful to the many people that helped me in this journey, and I am deeply grateful on having had the privileged opportunity of contributing to scientific advancement in an area I am passionate about, while experiencing the process of becoming a scientist.

The first acknowledgement undoubtedly goes to my main advisor Professor Omera Khan, who through her diligent, direct and supporting style has contributed more than she will ever know to my scientific education. I also thank Professor Jesper Larsen for his sustained, measured guidance through this PhD project.

I want to thank the wonderful people I worked with at the Massachusetts Institute of Technology: Jim Rice and Yossi Sheffi at the Centre for Transportation and Logistics, Hazhir Rahmandad and John Sterman at the System Dynamics group from the Sloan School of Management, and Nancy Leveson and John Thomas at the MIT Department of Aeronautics and Astronautics. Through them I thank their teams who gracefully navigated and guided my many questions.

I want to thank my friends and colleagues at DTU, starting with Christian who lured me to this corner of the world, and my travel team, colleagues and friends Anna, Katrin, Diana, Shahrzad, Martin, Samuel and Manuel, essential for making these years at DTU memorable.

Last but not least, I want to thank my family, who are my root, my foundation, and my unconditional supporters. A dedication goes here to them from this studious, curious traveller whom they helped create.

Abbreviations and acronyms

APICS	American production and inventory control society
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Control action
CAST	Causal analysis based on STAMP
CEO	Chief executive officer
CFO	Chief financial officer
CIA	Central intelligence agency
DDOS	Denial of service
DTU	Technical university of Denmark
e.g.	Exempli gratia, Latin meaning "*for example*"
ERP	Enterprise resource planning
FBI	Federal Bureau of Investigation
FMEA	Failure mode and effects analysis
FTA	Failure tree analysis
IAEA	International atomic energy agency
IC3	Internet crime complaint centre
i.e.	Id est, Latin meaning "*this is*"
IP	Intellectual property
HCS	Hierarchical control structure
IT	Information technology
ITM	Information technology management
MIT	Massachusetts Institute of Technology

NHS	National health service
OM	Operations management
PLC	Programmable logic controller
PR	Public relations
R&RM	Risk and resilience management
RSQ	Research sub-question
RQ	Research question
SC	Supply Chain
SCADA	Supervisory and control data acquisition system
SCM	Supply chain management
SCOR	Supply chain operations reference
SD	System dynamics
SLR	Systematic literature review
S&P	Standard & Poor
STAMP	Systems Theoretic Accident Model and Processes
STPA	Systems Theoretic Process Analysis
UCA	Unsafe control action
VO	Virtual organization
vs.	Versus
WEF	World economic forum

Table of Contents - Overview

Table of Contents - Detailed

List of Tables

List of Figures

1 Introduction

This chapter starts by outlining the industrial context surrounding this study and the factors that motivate this research. Thereafter the chapter derives the main research question from these motivating factors, and the initial research sub-questions that guide the literature review in the next chapter. This chapter then introduces some key terms that are used throughout this work and ends by presenting a brief outline of the structure of the thesis.

1.1 Research motivation

There has been an undisputed increase in the use of Information Technology (IT) in supply chains, with several indications that this trend is likely to continue (Da et al., 2014; Stevens et al., 2016; Gunasekaran et al., 2017). An effective response to market expectations requires activities that would be difficult or unfeasible to perform without the integration of IT systems to supply chain operations, for example:

- *A detailed plan, control and record of company activities*, whereby an ERP system (enterprise resource planning) is used to provide consistent access to real-time information throughout the organization. For example, a sports shoe manufacturer, upon receiving an order, uses an ERP system

to confirm product price, applicable customer discounts and credit history. At the same time, the order is filled from different locations simultaneously, the invoice is printed in any language the customer may require, the need for additional manufacturing workforce is identified, additional raw materials are scheduled, and successful product lines are identified for promotion (Edmondson et al., 1997),

- *Supply chain analytics systems*, whereby massive amounts of ever-changing data is analysed and interpreted. For example, after the September 11 New York attacks, Dell used its analytics systems to determine where supplies might be disrupted, increasing overseas production to mitigate anticipated shortages. At the same time, more efficient product configurations were identified to influence customers accordingly (Rocks et al., 2001),
- *Real-time inventory position monitoring*, whereby replenishment or real-time pricing can be controlled. For example, as Pepsi inventory in vending machines is depleted, the price per can is increased and the replenishment and procurement times are decreased (Webster, 2009),

The introduction of software into physical operations has allowed complex highly interactive and coupled processes to emerge, and it has been argued that "*programmable electronic systems have not introduced new forms of error, but by increasing the complexity of the processes that can be controlled, have increased the scope of the introduction of conventional error*" (Kletz, 1988).

Yet, at the same time, there has been an increase in the number of breaches that exploit this IT infrastructure causing behaviours for which it was not designed. It appears that the technology that allows a digital connectivity essential for activities society did not think possible before, is also the same infrastructure that is giving way to disruptions in the physical world (Webster, 2009, p.18), a phenomenon that is increasingly being identified as the supply chain's "cyber-risks" (Goldman, 2010).

The prefix "cyber" is used to "*describe a person, thing or idea as part of the computer and information age*" (Boyson, 2014), so in the context of this thesis and consistent with extant published literature (Warren et al., 2000; Hult et al., 2014), this term indicates a person, thing or idea where digital transmission and/or storage of information is involved.

In recent years, disruptions in the form of cyber-attacks to industrial organizations have affected national financial systems (Richards, 2014), electric power grids (Poulsen, 2009), nuclear facilities (Kushner, 2013), the movie and entertainment industry (Allen, 2014), and the retail industry (Reuters, 2014a) to name a few, making cyber-attacks a threat for many areas of the economy. As an example, foreign agents, by making use of the existing IT infrastructure, have even been able, remotely and anonymously, to render inoperable and tilt a floating oil rig, and delete records of containers at destination ports for the purpose of smuggling drugs (Reuters, 2014b).

The implications of a cyber-attack on the physical world reached an unprecedented level with the discovery of the Stuxnet attack on a nuclear enrichment facility located in Natanz, Iran. The foreign software that was found in the control systems of uranium enrichment plants was like nothing that had been seen before. It "tricked" the system into making its own equipment collapse.

The type of software to which Stuxnet belong are known as "worms", and have the ability to replicate without any external triggers. Stuxnet was highly specialized in as it used different stolen (and therefore fraudulent) identity certificates, and what was more striking, it used six "zero-day" exploits. A zero-day

exploit is a programming flaw that is first discovered by the user and the software manufacturer when it is exploited, i.e., used for the benefit of a foreign or unauthorized agent. As a reference, a computer virus would need just one “zero-day” exploit to be effective. Some computer viruses cause damage without the use of a “zero-day” exploit, as these are difficult to find, and as soon as they are detected, they are usually solved by through an update notification by the software manufacturer.

Stuxnet affected the control of an important piece of equipment in the process of uranium enrichment, called a centrifuge. Without getting into details of the enrichment process itself, it suffices to clarify that the centrifuge is a central component in the enrichment of uranium, and is an equipment that is required to spin at extremely high speeds, in the range of 100.000 revolutions per minute, an equivalent of 1600 spins every second. Controlling this speed is crucial both for maintaining a correct enrichment process, as well as for prolonging the life of the centrifuge, and since an enrichment facilities have over 8.000 centrifuges functioning at the same time, this is achieved through an automated control system (known as SCADA or Supervisory Control And Data Acquisition system) that has pre-programmed actions in case the

speeds are below or above safe operating speeds, known as operating thresholds.

Researchers found that Stuxnet obstructed the correct communication of the speed signal from the centrifuges to the SCADA: by passing an incorrect signal to the automatic controller of speeds below the required threshold, it caused the centrifuges to spin to speeds that eventually damaged them.

This iconic case brought several points to the public agenda.

- First, it became apparent that there are ways of severely affecting the physical world with software.
- Second, there are concerted efforts being made by groups with high technical know-how to disrupt operations through malicious software: the level of sophistication discovered in Stuxnet, suggested that it was not the creation of a lone programmer in his basement, but it required rather the effort, according to experts, of a team of at least 20 dedicated programmers over a period of at least six months.
- Third, there are little, if any, incentives to disclose when an attack had happened. Up to date, the Stuxnet cyber-attack has not been recognized by the Natanz uranium enrichment centre. It was rather detected via indirect information, in this case, the unusual replacement rate of centrifuges which

was being experienced in Natanz, as the trading of centrifuges for nuclear enrichment is monitored by international organizations such as the International Atomic Energy Agency (IAEA). Typically the replacement rate would be about 10% due to material damages or worker errors, yet during the time of the Stuxnet attacks, the replacement rose to as much as 25% (Zetter, 2014, p.3).

- Fourth, attacks might have been started long before they are detected. It has been estimated that Stuxnet had been in circulation and testing for at least five years before it was discovered in 2010.
- Fifth, there is an underground market of "zero-day" exploits, and in the black market, these can sell for as high as US$ 50.000 each. This has only been increased by the public disclosure of hacking tools through sites such as Wiki-Leaks.
- Sixth, malware can be advanced and built upon to create different varieties, as different varieties of Stuxnet have been identified since 2010, and it is as yet unclear if these are intermediate steps towards the final version that was discovered at Natanz or just simplified versions for other purposes.

- Seventh, even after years of expert decoding and analysis of the software that was found, there are still several unknowns. For example, the Stuxnet virus had the "turn off" date of 24 June 2012, the choice of the date unclear.

This was not the first case of digital sabotage, and there had been stories of the CIA implanting malicious software to sabotage the valves in a Russian pipeline as far back as 1982, presented at the time as a win-win situation, as even if it was discovered, the Russians would permanently be suspicious of digital technology from the west being described as "*a mission that would be successful even if compromised*" (Zetter, 2014, p.197).

With widely available technology, and connectivity through the internet, cyber-crime has become a widespread phenomenon. Despite underreporting being likely (Herrington et al., 2013; Onyeji et al., 2014), the Federal Bureau of Investigation (FBI) Internet Crime Complaint Centre (IC3) received 269.422 complaints in 2014 with overall complaints reporting losses of over US$ 800 million, corresponding to 46% of the complaints (IC3, 2017).

As a recent example, the "Wannacry" attack in May 2017 targeted computers of over 74 countries all over the world (Wong et al., 2017), taking data hostage until US$ 300 was paid to the

attackers. A solution to the continued spread of the attack was found only by chance. As an example of the effects, this attack affected as many as 70.000 devices in the national health system in the UK including computers, MRI scanners, blood storage refrigerators and operating theatre-equipment, forcing the cancellation of non-critical procedures, the turning away of non-critical emergencies, and the diverting of ambulances to other parts of the system (Foxx, 2017). This obtained substantive media coverage and has brought back the phenomenon of cyber-attacks to the forefront of public opinion.

The later "Petya" cyber-attack in June 2017, barely a month later, used a similar attack technique as Wannacry, and apparently build on the effectiveness of the attack, as no solution to its spread between computers was found, and an analysis of the virus code showed that even if the ransom was paid, the data would not be recovered (BBC, 2017). The only short-term solution that was found to prevent the data from being encrypted, was by shutting down the affected device if an unexplained restart was being experienced. Additionally, the email to which the ransom payments had to be confirmed was closed down by the hosting server, and thus no payments to the attackers were possible.

An example of the consequences of the Petya attack is the effects it had on the operations of the Danish shipping company A.P. Moller-Maersk, indicated at the time as one of the biggest disruptions to ever hit global shipping (Reuters, 2017). Petya caused the interruption of Maersk-run port operations in places such as Spain, the Netherlands, India and the United States, costing the company as much as US$ 300 million in lost revenue (Maersk, 2017). The society's infrastructure has never been as dependent as it is today on cyber activities working, yet, it has been argued that "*it is no longer a question whether an organization will be successfully hacked, but how long it will take to detect*" (Hult et al., 2014).

Cyber-attacks can cause considerable economic costs to the target companies and, in many cases, these costs and consequences are not noticed until after the damage has been done. Over one-third of companies that were affected by a cyber-attack in 2016, experienced a revenue loss of over 20% (Cisco 2017) and informed estimates report a 27,4 % yearly increase in the number of breaches from cyber-risks in 2017, costing organizations, on average, US$ 11.7 million (Richards et al., 2017). The likely annual costs from cyber-crimes anywhere from US$ 375 billion to US$ 575 billion in losses (Security & Mcafee,

2014). Furthermore, supply chain disruptions can, on average, reduce shareholder value by 7%, with effects even before formal announcements are made to the market by the affected company (WEF, 2013).

This is compounded by the increasing complexity of global supply chains, the speed and connectivity of operations required by companies to stay competitive, the growing skill of cyber-attackers to find novel ways of accessing crucial data (Reuters, 2012), and the limited information and tools available to manage these threats. This requires organizations to respond to cyber-attacks with increasing velocity and effectiveness, thus be more resilient, before their supply chains collapse during a cyber-attack. However, little is known about the methods for managing the resilience to cyber-attacks (i.e., cyber-resilience) in the supply chain.

There has been a lack of managerial action to acknowledge the relevance of the problem and find solutions (Burnson, 2013; Deloitte, 2012, 2013). It has been stated that "*only a few CEOs realize that the real cost of cybercrime stems from delayed or lost technological innovation*" (Bailey et al., 2014) and "*countries, like companies have likely underestimated the risk they face*" (Security & Mcafee, 2014). As a result, either by delayed

decision-making or by lack of awareness, the resulting inaction is leading to higher organizational costs from cyber-crimes.

The approach that is to be taken by supply chains to manage these disruptions is still a matter of debate. However, from companies that have taken steps to contain disruptions derived from cyber-risks, the evidence points to two main strategies: access control and financial hedging.

Access control is a strategy that has been pursued to safeguard processes and data through an increased investment in computer science technology, such as antiviruses, firewalls and cryptology (Windelberg, 2016). If a supply chain information network is thought of as a self-contained system, then access control approach restricts what can access this system (firewalls) detects any activity by foreign agents (antivirus) and confirms that the information that is exchanged between agents in the supply chain is accurate (encryption). All these activities can be considered as mitigation measures, to prevent disruption taking place derived from the existing IT systems.

Financial hedging, on the other hand, is used as a way of counteracting the effects of disruptions, by balancing these effects with some other equal but opposite transaction (Eggert et al., 2016). An example of this is the case of insurance. By paying a

premium i.e., cost of service, and if certain conditions are met the insurance company pays a pre-specified amount of money in case of a disruption derived from a cyber-risk. This is a common practice despite the many problems it creates and sustains.

Despite these approaches, companies continue to struggle in the solution to the problem of cyber-risks, as cyber-attacks continue to show that breaches circumvent existing measures, in industries that are "*in massive need for help, as they have no idea what the risks [from cyber-attacks] are*" (Wagstaff, 2014).

Linkov et al. (2013a) has mentioned the ability of a system to plan and prepare, absorb, recover and adapt to a negative event can be understood as resilience. For the case of cyber-events that require a resilient response, this response is a reflection of the cyber-resilience of the system. However, Linkov also mentions aspects which have hindered the identification of generalizable resilience principles, particularly the success of quantitative risk management, as "*pervasive concepts of risk have encroached the understanding of resilience*". Two issues stand out. First, resilience has a wider scope than risk, particularly when risk is incomputable, as in the case when the adverse conditions are unexpected or when the analytic paradigm has proven ineffective. This first issue is visible from the evidence gathered about cyber-

attacks in industry. Second, resilience has been fragmented into disciplines supporting incremental changes to known risks. This is at odds with the requirement to obtain a "*generalizable approach that is both applicable to a diverse array of systems and revealing of their interconnectivity*" (Linkov et al., 2013a). Resilience is therefore the relevant framework on which this research is based.

1.2 Thesis objective and research questions

An apparent contradiction between the expected management results from having risk management processes available and the increasing incidence of cyber-attacks is the foundation and the main objective of this work: the development of a scientific contribution towards the effective management of cyber-resilience through supply chain security and response.

The main research question of this thesis reflects the aspects described in the research motivation. Supply chains have had risk management processes for decades. However, there are records of an increasing number of incidents of operational disruption in supply chains caused by cyber-attacks. This work develops recommendations on how to manage the planning and recovery from operational disruptions resulting from cyber-risks in the

supply chain. Following the main objective of this thesis, the main research question is defined as:

> *Main Research Question (RQ): How can cybersecurity and cyber-resilience be managed in the global supply chain?*

In order to answer this complex question in a structured way, this work first lays out currently available knowledge on the topic of cyber-risk and resilience in the supply chain from the perspective of the intersection of three relevant knowledge domains:

- Supply chain management (SCM),
- Information technology management (ITM) and
- Risk and resilience management (R&RM).

The knowledge domain that concerns supply chain cyber-risk and resilience management can be understood as the intersection between these three knowledge domains as proposed by the following Venn diagram based on Khan et al., (2015).

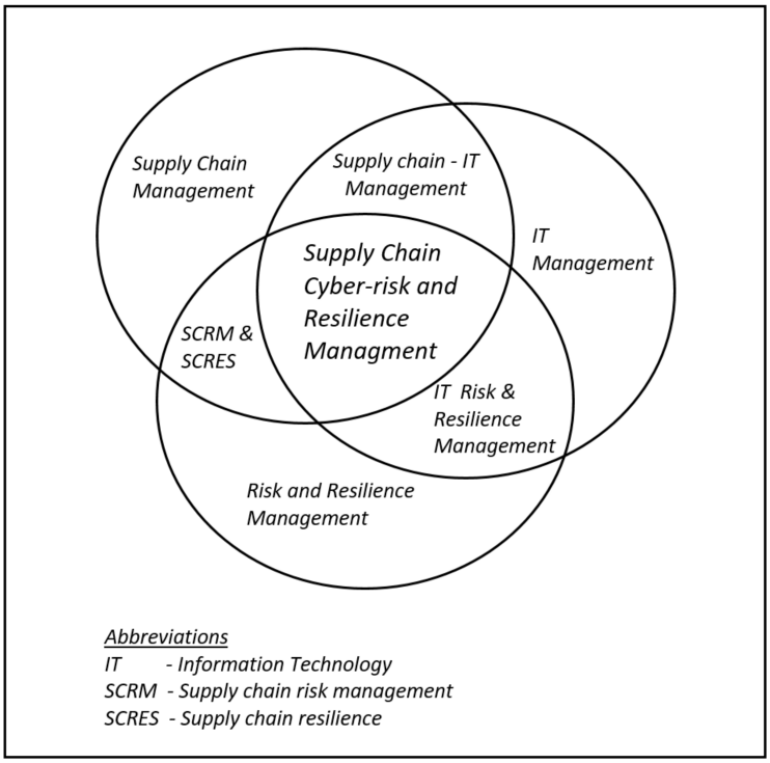

Figure 1 Relevant knowledge domains (Khan et al., 2015)

As shown in Figure 1, the base knowledge domains generate new knowledge domains that are even more relevant to the definition of the supply chain cyber-risk and resilience management knowledge domain. These are 1) supply chain IT management, 2) IT risk and resilience management and 3) supply chain risk and resilience management, and are the base of this work's review of current knowledge about the topic.

The first set of research sub-questions have been identified aimed at understanding the current state of knowledge about cyber-resilience in supply chains:

> *Research sub-question 1 (RSQ1): What are the supply chain cyber-resilience frameworks published in literature?*

> *Research sub-question 2 (RSQ2): Which case studies have been published about supply chain cyber-resilience with operational disruption?*

These two questions are directed at understanding both the available tools in literature for managing cyber-resilience, as well as the published cases of cyber-resilience with operational disruption. This information is obtained from existing published literature. The process for identifying relevant literature is described in chapter 0.

The literature review reveals gaps in existing literature. These gaps justify further research sub-questions necessary to answer the main research question. These derived research-sub-questions then guide the rest of this thesis research. Section 2.9 describes in detail the origin of these derived questions, research sub-question 3 (RSQ3) and research sub-question 4 (RSQ4). Figure 2 shows the research question and sub-questions considered in this thesis.

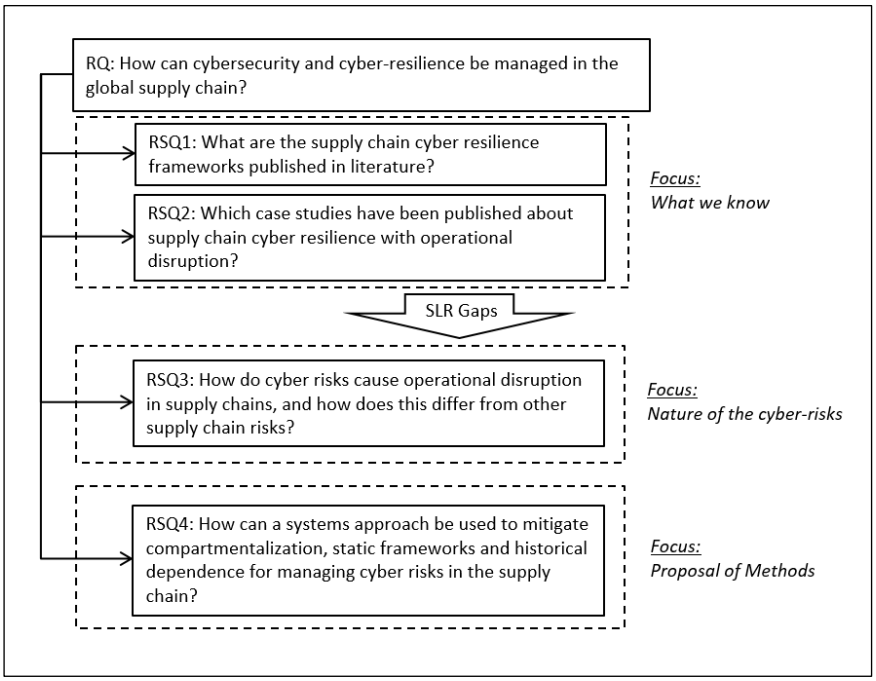

Figure 2 Main research question and research sub-questions

According to the previous figure, the thesis objectives and their respective research questions are laid out in Table 1.

Table 1 Objectives and research questions of this thesis

Objective	**Research Question**
Develop a scientific contribution towards the effective management of cyber-resilience through supply chain security and response	How can cybersecurity and cyber-resilience be managed in the global supply chain?
Identify and catalogue current knowledge about cyber-resilience in supply chains	What are the supply chain cyber resilience frameworks published in literature?
Identify and catalogue current knowledge of cyber-attack effects on supply chains	Which case studies have been published about supply chain cyber resilience with operational disruption?
Identify and catalogue the particular characteristics of cyber-risks in supply chains	How do cyber risks cause operational disruption in supply chains, and how does this differ from other supply chain risks?
Test and evaluate the use of systems thinking to address gaps in current cyber-risk and resilience methods for supply chains.	How can a systems approach be used to mitigate compartmentalization, static frameworks and historical dependence for managing cyber risks in the supply chain?

Before proceeding with the literature review, the next section first defines some terms that are used throughout this work, and the chapter ends by describing the structure of the thesis.

1.3 Definition of key terms

Some key terms are defined from the outset of this work to give a foundation of how these terms are understood and used in the thesis. This section does not provide a discussion of alternative definitions for these terms, as this research does not seek to define these terms better. Rather, the definition presented here serves as a foundation for further discussions and the development of aggregate or derived concepts.

Additionally, a glossary of terms is provided in the appendix of this thesis, with the definitions of several technical terms used in this thesis, mainly aimed at informing audiences from different backgrounds to whom this thesis is relevant, such as SCM, ITM and R&RM.

Hazard is considered "*a state or a set of conditions of a system that, together with other conditions in the environment of the system, will lead inevitably to an accident or loss event*" (Leveson, 1995).

Information technology (IT) is understood as the capabilities, tools and techniques involving the "*development, maintenance,*

and use of computer systems, software, and networks for the processing and distribution of data" (Merriam-Webster, 2017).

Risk is understood throughout this work as "*the possibility of loss or injury, through something or someone that creates a hazard.*" (Leveson, 1995).

The supply chain is be understood as "*the network of organizations that are involved, through upstream and downstream linkages, to the different activities that produce value in the form of products and services delivered to the ultimate consumer*" (Christopher, 2011, p.13).

Supply chain management (SCM) is understood as the "*management of upstream and downstream relationships with suppliers and customers in order to deliver superior customer value at less cost to the supply chain as a whole*" (Christopher, 2011, p.3).

1.4 Structure of the thesis

This thesis is divided into nine chapters in addition to a reference and appendix. Through this structure, the sequence of enquiry for answering the research question and sub-questions is laid out sequentially, and the methods, results and supporting documentation are described, as explained next chapter by chapter.

Chapter 1 outlines the industrial context for this study, describes the factors that motivate this research, by introduces the main objective and research question of the thesis, presents the initial research sub-questions that motivate the literature review, and introduces key terminology.

Chapter 2 describes the method, process and results of a systematic literature review carried out to gather and analyse published literature about the topic of cyber-risk and resilience in the global supply chain. The analysis of the gathered data identifies gaps in the extant literature that prevent answering the research question. These gaps give rise to additional research sub-questions which are mentioned at the end of the chapter.

Chapter 3 describes the methodology used in this thesis by defining the philosophical position of this research from the ontological, epistemological and axiological dimensions. The research design is then presented and descriptions are given for the chosen research approaches for answering the research questions, i.e., a documentary / archival research process, a systems approach to risk assessment, and a dynamic simulation.

Chapter 4 describes the results of the research process to address the first research sub-questions derived from the identified literature review gaps, related to the "*nature*" i.e., the particular characteristics of cyber-risks, by analysing data about cyber-attack reports.

Chapter 5 describes the results of the research process to address part of the second research sub-question derived from the identified literature review gaps, related to the use of systems thinking to evaluate cyber-risks. The chapter presents the results of the systemic risk analysis approach as applied to in-depth cases

in the United States. The performance of this method is then compared to a traditional risk assessment method.

Chapter 6 describes the results of the research process to address the remaining of the second research sub-question derived from the identified literature review gaps, related to the use of systems thinking to evaluate cyber-resilience. The chapter presents the results of a system dynamics model developed for a detailed case study.

Chapter 7 analyses the results in chapters 4, 5 and 6 in a discussion towards answering the research sub-questions laid out after the systematic literature review in chapter 2. Finally, this chapter answers the main research question of this thesis, based on the research results.

Chapter 8 describes and categorizes the contributions made throughout this thesis, both from the perspective of academia and industrial practitioners.

Chapter 9 presents the conclusions for this thesis, summarizes the process followed in this work, reviews the research question and sub-questions with their answers, and derives potential future areas of research.

1.5 Summary of the chapter

This introduction described of the industrial context for this study, and the factors that motivate a research about managing cyber-risk and resilience in the global supply chain. Furthermore, this chapter introduced the main research question as derived from these motivating factors and the initial research sub-questions that motivate the literature review in the next chapter. This chapter then gave a definition of some key terms used throughout this work and closed by presenting a brief outline of the structure of this thesis.

The next step in this work, based on the initial research sub-questions, describes the current state of knowledge about cyber-risks, by reviewing extant literature on the topic.

2 Literature review

This chapter first gives a background about the process of a literature review and describes the suitability of carrying out a systematic literature review in particular. The chapter then identifies the biases present in the review process and outlines the choice of systems thinking as the framework through which the literature review analysis is carried out.

This chapter goes on to detail the systematic literature review method and presents the results of the application of this method, first in descriptive terms detailing aspects such as the number and sources of the selected documents, and then thematically.

Finally, the initial research sub-question RSQ1 and RSQ2 are answered, relevant gaps found in the literature are outlined, and the remaining research questions and strategy of enquiry is completed, which the rest of this thesis proceeds to answer.

2.1 Literature review background

A literature review is an attempt to make inferences based on the consideration and analysis of studies by other researchers. It is considered as the "*identification, synthesis and assessment of all available evidence, quantitative and/or qualitative in order to generate a robust, empirically derived answer to a focused research question*" (Mallett et al., 2012).

A literature review is a first step towards understanding the state of the knowledge in a specific field, which for this thesis is the knowledge regarding cyber-risk and resilience for the case of supply chains. A literature review process avoids "*reinventing the wheel*" (Zorn et al., 2006), integrates existing knowledge through the accumulation of scattered and potentially unconnected research, and revitalizes the development of knowledge (Webster et al., 2002).

Medical science was one of the earliest areas to systematize the concept of advancing scientific knowledge through the collection and synthesis of scientific work by others. Murlow (1987) introduced guidelines to make the process of gathering and evaluating literature more systematic, i.e., reproducible, and is one of the earliest suggestions of an approach that has come to be known as "Systematic Literature Review" (SLR).

The SLR constituted an improvement from what was a classical literature review based on a more narrative approach, with no specific methodology or structure. SLR reflects an incremental development of the review process towards reproducibility, transparency and comparability, and thus a more positivist approach to literature reviews (Jesson, 2011).

From medicine, SLR has been adopted by other fields of research and adapted to the more specific needs of these fields, including management (Tranfield et al., 2003), software

engineering (Brereton et al., 2007), supply chain sustainability (Teuteberg et al., 2010) international development (Mallett et al., 2012), and more recently, SCM (Durach et al., 2017).

Literature reviews have been acknowledged as playing a central role not only in the accumulation but also in the creation of knowledge (Webster et al., 2002; Boell et al., 2014; Jennex, 2015). Ways in which a literature review creates new knowledge include: the synthesis or conversion of existing knowledge, theory building that would need to be validated in future research, adoption of new viewpoints or concepts at a different level of aggregation, theory testing in the case where a number of empirical studies have been accumulated, the identification of research gaps, and through the provision of research agendas (Schyren et al., 2015).

The process of knowledge creation through SLRs is relevant in some areas. For example, in 2016, SLR constituted more than 40% of the publications for the journal Nature Reviews Immunology, with 48 articles out of a total of 116 published during that period (Durach et al., 2017).

2.2 Relevance of a systematic literature review

A systematic literature review is a special type of literature review that uses an explicit method and comprehensive strategy that has been defined before the review takes place (Denyer et al.,

2009). The relevance of a systematic approach to literature reviews is reflected in the structure and social significance of its final results, with implications for explicitness, transparency, comprehensiveness, trustworthiness, relevance, and synthesis of the results.

First, a systematic approach makes an explicit description of the protocols used before the actual data collection starts. This helps to reflect and reduce hidden bias in the data collection process. The philosophical position of the research determines if and to what extent the researcher is a subjective or objective part throughout the research process. Greater bias is expected for a subjective researcher position, and less so if the researcher position is more objective. Yet, regardless of the level of accepted bias in the research process, an explicit description of the process creates greater transparency and improves reproducibility and comparability.

Second, through the use of explicit protocols, a systematic approach creates transparency about how the analysis is carried out and how the conclusions are generated. This reduces the misrepresentation of the available knowledge collected for the review, promotes critique that is more focused, and results in more efficient improvement of any future SLR process.

Third, a systematic approach attempts to gather as much of the available research as possible by reducing the excessive influence

of studies that are simply easier to find through the use of inclusion criteria. Inclusion criteria describe the way in which to assess how much each study addresses the research question. A systematic review does not need to be exhaustive as some reviews only attempt to gather representative examples of evidence to answer the research question. These types of reviews benefit nonetheless from being explicit in their criteria.

Fourth, a systematic approach to a literature review indicates to the reader how much the conclusions reached by the review can be trusted, i.e., its validity. Science is not only the advancement of the contents of the available body of knowledge but also the process of its diffusion and acceptance by relevant communities (Resttvo, 1988). This makes trust on the results reached by systematic reviews a fundamental part of the research process objectives.

Fifth, as a way of increasing the acceptance of the findings, a systematic approach should include information from relevant communities of interest to the research question.

Finally, a systematic approach presents a synthesis of the results in the form of a structured narrative, summary tables and some type of meta-analysis such as statistical indicators. This analysis then drives recommendations intended to connect the findings from the information that was gathered and the conclusions derived by the researcher.

2.3 Bias in the structured literature review

It is unlikely that an SLR is without error as, at the very least, the human nature of the scientists performing the research introduces biases into the SLR process. Biases in SLRs are reflected as discrimination or prejudices against some results in favour of other results and are thus considered systematic errors, i.e., errors which present themselves consistently in a similar way. This is in contrast with random errors, where the error source is unknown and can vary in any direction.

Systematic literature reviews contain different biases that need to be identified and controlled to increase the objectivity, validity and transparency of the results. Biases present in SLR have been described in the literature as either related to the search space (sampling bias), the search tool and the tool user (selection bias), the objective processing of the gathered data (within-study bias), or the subjective processing of the gathered data (expectancy bias).

The first main bias is sampling bias. Felson (1992) defined it as the possibility of being unable to retrieve all the relevant findings on the aspects that are required by the relevant research questions. This bias is connected with the search space where the information is located and is composed of two other biases that drive it.

The first constituent of the selection bias refers to the possibility that the relevant findings might not necessarily be available for retrieval (regardless of how thorough the retrieval process is) due to discrimination at the journal editing board, that might decide against the publication of results that challenge existing knowledge, results that are negative (i.e., results do not confirm a hypothesis), or results that confirm existing knowledge (reproducibility studies). This is known as "*publication bias*".

An example of publication bias is the existing discrimination towards publishing positive results only, having grown as much as 22% in areas of social science research in the last 20 years, with effects that are particularly burdensome to the scientific process (Fanelli, 2011; Granqvist, 2015). A positive result is when the expected or wanted effect of an experiment was indeed observed. Despite positive results being the most attractive of the possible outcomes, a negative result also holds important information, and not sharing this through publication leads to inefficient use of resources through the lack of shared insights. The scientific community could thus potentially be making the same mistake over and over again instead of trying new ways of conducting the experiment.

The other subcomponent of the sampling bias relates the inability to access a representative sample of the available literature on the subject, i.e., "*retrieval bias*". This is partly driven

by the publication bias (Daniels, 2002), and by an incomplete search protocol lacking a mix of search engines that cover the relevant area of study.

The second main bias is the "*selection bias*", defined by Felson (1992) as the possibility for the search resulting in an incomplete or wrong subset of relevant literature for analysis. This bias refers to the search process itself and the researchers performing the search and is also composed of two biases that drive it. The first pertains to the inclusion criteria that were chosen to identify relevant literature, as these criteria might be incomplete when based on defective theoretical boundaries, units of analysis or sources of data. This bias is known as "*inclusion criteria bias*". The second constituent of the selection bias pertains to the subjective application of the inclusion and exclusion criteria by the researcher or researchers performing the search, known as "*selector bias*". These biases are based on two complementary aspects: having the correct tool as represented by the inclusion and exclusion criteria, and using the tool correctly.

The third main bias is the "*within-study bias*", defined as the potential variability in the coding of the documentation that has been retrieved (Durach et al., 2017). Coding is the process through which the gathered data is classified, grouped and/or ranked. The coding results in the identification of the relevant constituent parts for each of the pieces of data that were chosen during sampling,

and the subsequent integration and grouping of these constituent parts in a way that may answer the research questions that justified the SLR. Despite coding being necessary to facilitate the analysis towards answering the research questions, the approach through which these constituent parts are grouped highly depends on the experience of the research team and considers aspects such as the philosophical framework applied in the analysis.

The fourth main bias is the "*expectancy bias*", defined as the possibility that the research team discriminates against information that is perplexing, thus rather going for the information that conforms to their expectations (Durach at al., 2017). This bias can be understood as the subjective processing of data. Different forces are at play when this bias is present such as the pressure to publish positive results (as was discussed in the sampling bias), which could lead to discarding outliers or data that leads to negative results, or the inexperience of the researchers, which could lead to prematurely considering unexpected data as errors from the sampling process.

This thesis has taken three measures to mitigate the sampling bias through its two sub-components: first, by working with several search engines relevant to the topic; second, by seeking the advice of specialist librarians both at the Technical University of Denmark (DTU) and at the Massachusetts Institute of Technology (MIT) to confirm the most reliable sources of

information for the search; and third, by considering a variety of source for published literature, i.e., peer-reviewed journals, book chapters and conference papers.

Additionally, this thesis has taken three measures to mitigate selection bias, within study bias and expectancy bias. First, more than one researcher was involved in the generation of the search criteria, to ensure different opinions on search terms and combinations. Second, the search was done in 2015 and updated in 2017 to include more recent literature, updated results based on revisited and adjusted search criteria. Third, the literature review was subject to a peer-review process as part of a paper submission to a peer-reviewed journal, to obtain feedback regarding the suitability of the applied keywords and search strategy.

Finally, this thesis has taken one additional measure to mitigate the within-study bias, by defining systems thinking as the underlying ontology and resulting framework through which the coding is carried out. The foundations of systems thinking are explained at length in the methodology chapter and the next section describes the principles of systems thinking, to understand the choice for its use during the SLR coding process.

Table 2 shows a list of the different biases present during a literature review process, their definitions, the proposed mitigation strategies suggested in the literature, and the mitigation strategies included in the literature review of this thesis.

Table 2 Biases in the Systematic literature review process

Bias type		Definition	Proposed mitigations	Mitigations used in this work
Sampling bias		Failure to retrieve all relevant study findingson the aspects of the developed theoretical		
	Retrieval bias	It is the risk that the chosen sample is not representative of the available literature base	Commisioning of expert searchers who understand databases and search	Use of a variety of search engines. Use of advice from Librarians at DTU and MIT
	Publication bias	Discrimination by journals to favor publishing results that challenge or change existing knowledge, while studies that confirm previous knowledge are	Consider both published and unpublished sources (Tranfield et al., 2003). Consider journals that	Use of published sources from high quality journals. Inclusion of non published sources.
Selection bias		Risk of search resulting in the incomplete or wrong subset of relevant		
	Inclusion criteria	Inaccurate design of selection criteria: Theoretical boundaries, unit of analysis, sources of data, and study contexts.	Parallel and independent development of inclusion/exclusion criteria by two or more researchers	Use of multiple researchers and review process
	Selector bias	Subjective application of inclusion/exclusion criteria (Cohen, 1960)	Involvement of multiple researchers and use of blind processes, where researchers do not have access to journal or author names during selection process	Use of multiple researchers and review process
Within-study bias		Risk of the variability in the coding of primary studies retrieved in the SLR (Durach et al., 2017)	Involvement of multiple independent coders (Felson, 1992), Involvement of an	Use of multiple researchers and review process
Expectancy bias		Risk of researchers discriminating information that is perplexing and favoring information that conforms to their	Involvment of multiple coders from different sociocultural and educational	Use of multiple researchers and review process

2.4 System thinking as coding framework

A coding framework provides the criterion through which the descriptions, categorizations and discussion derived from the data obtained for an SLR, are presented. This framework makes the data comparable, and facilitates the identification of gaps in this data with respect to the research questions that the SLR answers. The choice and description of systems thinking as a coding framework is explained next.

A system is a "*regularly interacting or interdependent group of items forming a unified whole*" (Merriam-Webster), where "*the system is something more than the collection of its parts*" (Meadows, 2008). Systems thinking is thus an approach to related concepts, methods and tools for understanding the world from the perspective of the systems from which it is built, and it is thus a "*system for thinking about systems*" (Arnold et al, 2015).

From the description of the problem laid out in the introduction of this thesis, a visible characteristic a global supply chain is the multitude of systems interact due to the use of information technology (IT) within a competitive market. Such systems include

- IT-hardware systems,
- IT-software systems,
- Organizational systems,

- Physical systems such as warehouses and transportation,
- The interaction of these systems within each of the different agents in the supply chain, and
- The interactions of the agents -systems in themselves- with each other.

As interdependence increases and networks get larger, it is "*not good enough to get smarter and smarter about our particular piece of the rock*" (Richmond, 1994), and a common language becomes necessary for sharing knowledge between the different interacting parts. The systems thinking approach thus becomes an option for making sense of this complexity (Meadows, 2008; Plate, 2010; Sterman, 2003; Senge, 1990).

Different definitions of systems thinking have been offered in the literature. Peter Senge defined systems thinking as "*a discipline for seeing wholes and a framework for seeing interrelationships rather than things, for seeing patterns of change rather than static snapshots*" (Senge, 1990), while Barry Richmond defines systems thinking as "*the art and science of making reliable inferences about behavior by developing an increasingly deep understanding of underlying structure*" (Richmond, 1994). Sweeney and Sterman have defined systems thinking as "*the ability to represent and assess dynamic complexity, e.g., the behaviour that arises from the interaction of*

a system's agent over time, both textually and graphically" (Sweeney et al., 2000).

More recently, Arnold et al., (2015) developed a unified definition that considers aspects of systems thinking by different authors.

"*Systems thinking is a set of synergistic analytical skills used to improve the capability of identifying and understanding systems, predicting their behaviours, and devising modifications to them in order to produce desired effects. These skills work together as a system*" (Arnold et al., 2015).

Literature presents different applications for systems thinking in diverse fields concerning SCM with different levels of aggregation. A level of aggregation is understood as the grouping or collections according to which a phenomenon is described and studied. A higher level of aggregation takes a broader view and thus makes analyses that describe a phenomenon according to some larger grouping criteria. For example, an analysis of cyber-risks at a country level is said to have a higher level of aggregation that an analysis of cyber-risks at a company level.

Systems thinking has been used for understanding complex problems in areas such as production control (Forrester, 1960; Sterman, 2000, p.710), project management (Jalili et al., 2016), claims settlement in complex projects (Cooper, 1980), commodity market analysis (Glöser-Chahoud et al., 2016), healthcare (Vennix

et al., 1992; Homer et al., 2006; Peters, 2014), oil industry (Morecroft et al., 1992), worker burnout (Homer, 1985), maintenance (Sterman, 2000, p.66), antibiotic resistance (Homer et al., 2000), biomedicine (McCarthy et al., 2014), automobile leasing industry (Sterman, 2000, p.42), agriculture and natural resource management (Turner et al., 2016), and humanitarian logistics (Besiou et al., 2011).

The use of systems thinking for analysis, sense-making and knowledge development in an SLR requires defining the epistemological framework, i.e., what is considered as knowledge at the time of the analysis. The systems thinking framework is derived from the definitions that are available in the extant literature, and conditions the way in which the information gathered in the SLR can be organized. Although the different aspects concerning systems thinking are explained in the methodology section, three aspects are considered for the SLR analysis 1) the "*leverage level*" of the framework, 2) the feedbacks present, and 3) the level of aggregation for each resilience framework.

The first aspect of the analysis framework is understanding and identifying the "*leverage level*" for each of the cyber-resilience frameworks identified in the SLR. The leverage level is the degree of abstraction that is taken to understand a system. In the systems thinking perspective, the understanding of systems can take place

at different levels. A first level is through the behaviour of the system, i.e., what is apparent and can be observed or recorded. A second level would be through the patterns of behaviour present in the system, which results in the specific behaviours seen in level 1. A third, deeper level is through the structures that cause the patterns which in turn cause the behaviours of the system. Changes in this third level are typically the most efficient, creating a bigger and more enduring change for the same unit of cost, than at any of the other two levels, and is thus said to be the level with the highest leverage.

The analysis of the SLR with the use of a systems thinking framework consists of identifying the elements that compose each these frameworks and their connections, and to explain an observed behaviour such as a performance measure. The gathered data contains a number of resilience frameworks, with potential relationships between these (some might have been derived from others), and the performance measure is of how relevant these frameworks are for managing cyber-risks in global supply chains.

In order to understand the system leverage, the systems thinking framework considers 1) an analysis for each of the resilience frameworks in the SLR data with respect to the components of the framework, and the proposed relationships between these components, 2) a categorization of the resilience

frameworks with respect to the aspect they address, a behaviour, a pattern or a structure in the system.

The second aspect of the analysis framework is understanding and identifying the feedbacks present in the resilience frameworks that have been identified. A feedback structure is a chain of circular causality that results in changes over time of a variable of interest, i.e., the dynamic behaviour of the system performance. A relationship between elements in a system is considered causal if it is "*sequential in time and incorporates some hypothesis about the mechanisms whereby one element directly influences another*" (Meadows et al., 1985, p 11).

Thus, for resilience frameworks the "feedback" analysis aspect considers 1) identifying feedback, i.e., circular causality, and structures, i.e., elements and connections, and 2) categorizing the different resilience frameworks as static or dynamic in terms of how the framework conceptualizes supply chain cyber-resilience.

The third aspect of the analysis framework relates to understanding the level of aggregation for cyber-resilience in each of frameworks. Different levels of aggregation i.e., grouping of the elements and connections that make up the structure of a system, influence aspects of the analysis process such as the categorizations of the information that is necessary to implement the framework and the unit of analysis that would be involved.

For cyber-resilience frameworks, the "*aggregation*" analysis aspect considers identifying 1) the unit of analysis for each of the resilience frameworks, 2) level of aggregation for the information needed to implement the framework.

Figure 3 summarizes the aspects of systems thinking included in the framework for analysing the literature review.

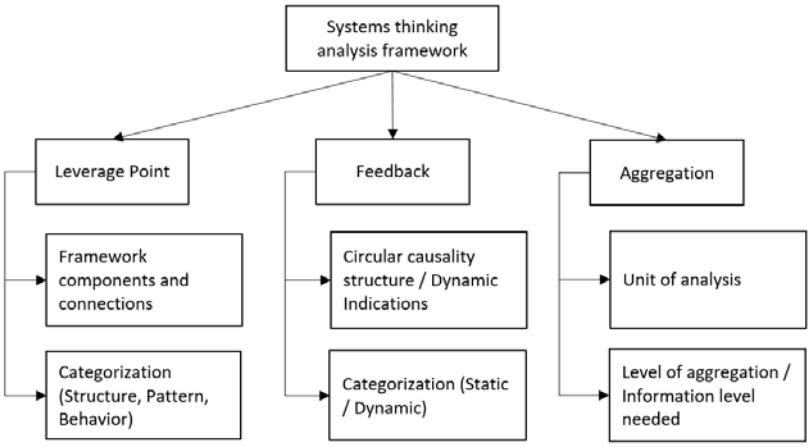

Figure 3 Aspects in a systems thinking analysis framework

This thesis has so far described the need and suitability of an SLR, it has described the potential biases in the SLR process, outlining mitigation measures included in the process to mitigate these biases, and it has described the systems thinking framework applied in the SLR analysis. The following sections describe the SLR process in detail.

2.5 Methodology for the systematic literature review

The systematic literature reviews in this thesis were conducted based on documented guidelines for the management discipline as outlined by Durach et al., (2017). Durach builds on both the frameworks by Murlow (1987) for the medical field and its adaption to management by Tranfield et al., (2003). The paper outlines the idiosyncrasies present in SCM research, and the biases present in the systematic literature review process.

Tranfield identified differences between of management and medical research according to twenty different dimensions. These differences range from the nature of the disciplines and the resulting data extraction and synthesis practices to the reporting and implementation of evidence. In particular, Tranfield argues that medical research has a great degree of convergence in regard the to what the field considers as important, and as a result 1) the research questions are clearly defined, 2) the scope of the research is geared towards interventions that deliver results, 3) the research is predominantly quantitative, 4) the research presents a tradition of meta-analysis and structured reviews, and 5) results are presented with a standardized report structure.

On the other hand, management research has traditionally been characterized by divergence in terms of what the discipline finds important, as an increasing number of areas are being addressed through management research. This results in management

research 1) presenting a low consensus about what the research questions should be, 2) delivering both qualitative and quantitative results, 3) concerning itself with why something works and the contexts where these benefits happen, 4) presenting the results in the narrative, and 5) using non-standardized report structures.

The systematic literature review chosen for this thesis is a comprehensive, explicit and reproducible six-step method for the identification and analysis of appropriate documents and publications, aimed at answering specific research questions (Durach al., 2017). The six steps of the SLR process are grouped into three phases, as shown in Figure 4, and are explained in detail next.

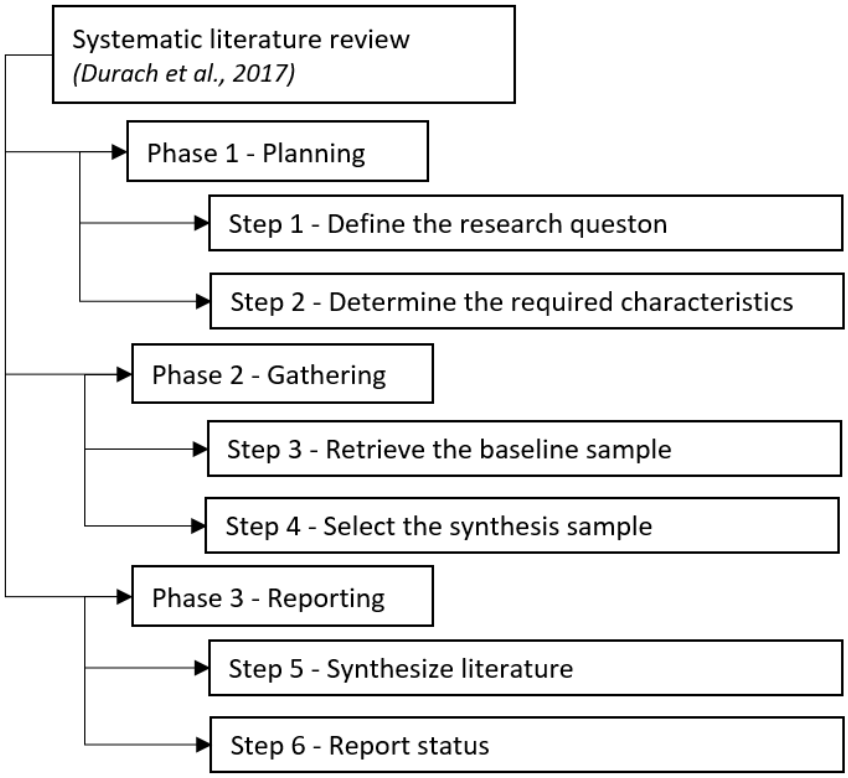

Figure 4 SLR process (based on Durach et al., 2017)

2.5.1 Phase 1 – Planning the review

The planning phase for an SLR is a process that results in a list of characteristics that justify the need and guide the application of such a review. The need for an SLR is justified through an argument about the relevance of the SLR as a way of answering a relevant research question. The guide to the application of the SLR is determined by a list of characteristics and requirements for

the SLR process, and which the gathering phase implements. Durach et al., (2017) proposes the planning can be structured in two sequential steps: first, define the research question and the suitability of SLR for answering this research question, and then create a protocol to explicitly define the process through which this SLR is carried out.

Step 1: Define the research questions. In this step, the studied phenomenon is described to identify the scope of the literature review as resulting from research questions. Thereafter an argument is given as to why a literature review is an appropriate way of answering these research questions.

The planning process is considered an iterative process of definition, clarification and refinement (Clarke et al., 2004). The result is a number of research questions that are considered valuable and which respond to the gap found in the current theoretical framework for a specific context, as illustrated in the following figure.

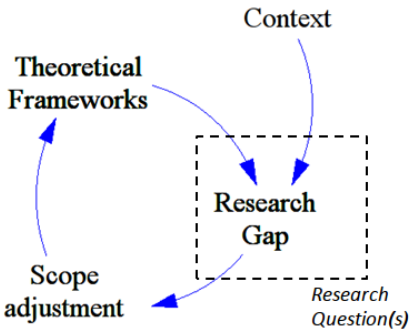

Figure 5 Review planning (based on Tranfield et al., 2003)

The following research sub-questions (RSQ) were laid out in the introduction chapter:

> *Research sub-question 1 (RSQ1): What are the supply chain cyber-resilience frameworks published in literature?*

> *Research sub-question 2 (RSQ2): Which case studies have been published about supply chain cyber-resilience with operational disruption?*

As all these questions are concerned with the existing knowledge about cyber-resilience frameworks and the risks themselves, a review the extant literature is suitable for answering these questions.

Step 2: Determine the required characteristics. This step consists in defining the criteria 1) for selecting the documents used for answering the research questions, and 2) for the search process for identifying those documents. The documents criteria define both what is to be included in the sample and what is to be excluded from the sample. The criteria for the search process define how the work is carried out, where the search is performed, and what form the search patterns take. These criteria are reflected in a document known as the "*SLR protocol*".

The SLR protocol is an action plan for identifying and selecting documents to answer particular research questions. The main purpose of the SLR protocol is to maintain the objectivity of the results by describing all the steps taken in the review process. The main components of the SLR protocol are the 1) context for the study, 2) the research question or questions, 3) an indication of the value of carrying out the SLR, 4) the sources for the data, 5) the search strategy and 6) the inclusion and exclusion criteria (Durach et al., 2017).

The first three components of the SLR protocol, namely the context of the study, the research questions and the value of

performing an SLR have been argued during the first part of this chapter and during the introduction. The rest of the components are defined next. A summary of these components is shown in Table 3.

The fourth component of an SLR protocol are the *sources of the data*. These have been defined as search engines for published scientific peer-reviewed literature. Four research databases are considered in this SLR. These databases were identified from meetings with reference librarians at DTU and MIT. The chosen databases are:

- Web of Science (https://apps.webofknowledge.com)
- EBSCOhost (https://search.ebscohost.com)
- ProQuest (https://search.proquest.com)
- Google Scholar (https://scholar.google.com)

The fifth component of the SLR protocol, the *search strategy*, defines the parameters that will condition the search process a) the search keywords, b) the search patterns, c) the unit of analysis, d) the language of the publications, and 4) the years publication for the documents.

The *search keywords* were determined from a knowledge domain analysis of the concept of supply chain cyber-risk and resilience, as represented in Figure 1. The three main knowledge domains to be considered were identified as “supply chain management”, “information technology management”, and “risk

and resilience management". This analysis defines the main keywords that are used in the systematic literature search. Table 3 lists the keyword used in the systematic review.

Table 3 Keywords and search terms used in the systematic review

Concept	**Keywords**
Supply chain	Supply Chain
	Supplier
	Supply Network
	Supply Chain Management
Cyber	Cyber disruption
	Cyber resilience
	Cyber risk
	Cyber attack
Information Technology	Information Technology
	IT
Risk and Resilience	Disruption
	Disruption Management
	Resilience
	Resilient
	Resiliency

- The search *patterns* are the different keyword combinations used for identifying documents in the search engines. These patterns are defined by three rules: 1) The concepts are combined through AND operators, 2) The keywords within each concept are combined with the OR operator, and 3) At least 2 concepts are included. Figure 6 illustrates the search pattern structures.

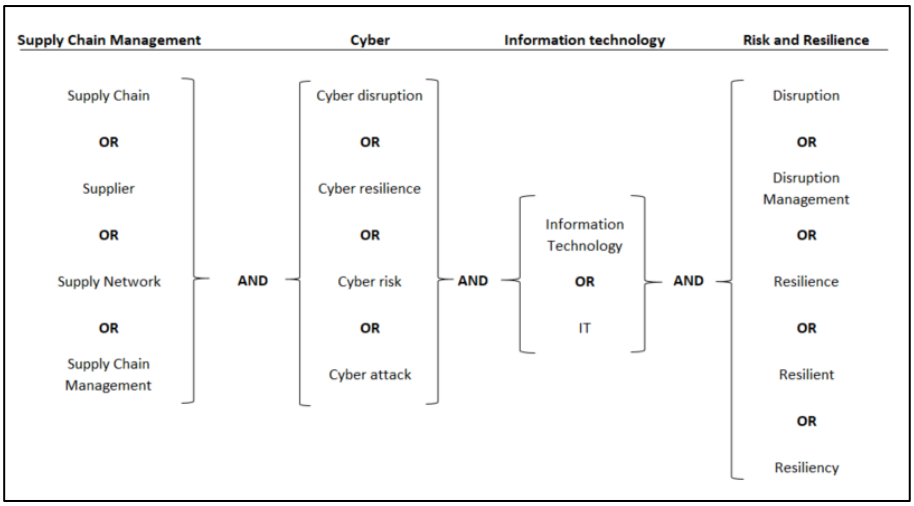

Figure 6 Search pattern structures

- The *units of analysis* that is considered for this literature review are published, peer-reviewed articles and peer-reviewed conference papers.
- The *language of the articles* considered is either English, German or Spanish, as these are the languages spoken by the thesis author.
- The *years of publication* for the literature research are papers between the years 1985-2017.

The last component of the SLR protocol, i.e., the *inclusion and criteria*, is necessary to narrow the number of papers that result from the search engine to a baseline sample. Following an analysis of the title and abstract of the documents from the initial search results, the baseline sample will include documents that meet the following criteria:

- Document is about supply chains or relevant to supply chains
- Document is about the recovery of operations from unforeseen disruptions
- Documents presents a framework to structure decision-making
- Document considers the information exchange and storage in the analysis

The research protocol gathers the information that has been described in this section and is shown next.

Table 4 Research protocol for literature review

Relevant Theoretical frameworks SLR	Systematic Literature Review (Durlach et al., 2017)
Context for research	Cyber attacks continue to occur in suply chains. Yet, Supply chains alrady consider risk management in some ways. This apparent contradiciton is the source of a research gap.
Relevance of a Systemtic Literature Review	A review of the current published information about resilience frameworks and their applicability to cyber-risks, can highlight areas where there is an opportunity for research.
Unit of Analysis	1.- Published, peer-reviewed articles 2.- Reports by International organizations, agencies and consultants
Research Question	RSQ1: What are the supply chain cyber resilience frameworks published in literature? RSQ2: What cases have been published about supply chain cyber resilience with operational disruption? RSQ3: How do cyber risks cause operational disruption in supply chains? RSQ4: How do cyber- risks differ from other supply chain risks?
Sources of Data	International search engines for acadmic articles and reports from the year 1985 to the present; articles in English.
Search Strategy	Peer reviewed articles - Triple filtering approach A.- Use selected "Search Engines" with the "Keyword combinations" to obtain a first selection of documents. B.- Review references in documents chosen in A.- to identify other relevant documents by using the "Topic Relevance Criteria". C1.- Peer reviewed articles - Review abstracts of documents chosen in A.- and B.- to identify relevant documents for analysis by using the "Topic Relevance Criteria" C2.- Other Documents - "Identify Trustworthiness Factors" and "Topic Relevance Criteria" to filter relevant documents
Inclusion Criteria	Search engines: Google Scholar, Web of Science, EBCOhost, ProQuest Keyword Combinations: (Supply chain OR Supplier OR Supply Network OR Supply Chain management) AND (IT OR Information Technology) AND (Resilience OR Resilient OR Resiliency OR Disruption OR Disruption Management) AND (Cyber disruption OR Cyber resilience OR Cyber risk OR Cyber attack) Topic Relevance Criteria: *Document is about supply chains or relevant to supply chains, *Document is about the recovery of operations from unforeseen disruptions, *Document presents a framework to structure decision-making *Document considiers the information exchange and storage in the analysis

2.5.2 Phase 2 - Gathering the data

The process of conducting the literature review is carried out according to the protocol defined in the first phase. The gathering phase according to Durach et al., (2017) is to be carried out in two steps of increasing scrutiny: first with the selection of a broad sample from a partial analysis of the documents, i.e., the "*baseline sample*", and subsequently a refined smaller set of documents following a thorough review of the documents, i.e., the "*synthesis sample*".

Step 3: Retrieve a baseline sample. This step considers the identification of the sources according to the search strategy. This is done with the chosen search engines by applying keyword combinations defined in the protocol. The title and the abstract of the resulting papers are reviewed according to the inclusion and exclusion criteria to form the baseline sample. This step also considers the identification and elimination of duplicates, as the same article might be a result of searches using two different keyword combinations.

Step 4: Select the synthesis sample. This step considers refining the documents found in the previous step through two main processes. First, the baseline sample is refined by testing of the relevance of the publication based on the content of the whole document beyond the title and abstract. Second, the references to the refined set of articles are reviewed to identify relevant

documents that might not have been identified through the initial broad search. The set of documents that results from these two processes is called the “synthesis sample”.

2.5.3 Phase 3 - Reporting the results.

The reporting phase according to Durach et al., (2017) considers the synthesis of the sample according to a specific framework, in addition to the status reporting of the findings.

Step 5: Synthesize literature. This step considers the extraction of data from the synthesis sample, according to both the characteristics of the publications themselves and the theoretical framework for the analysis. Furthermore, the step considers the integration of this data into proposals of how the initial theoretical framework can be refined, the identification of the mechanisms described in the sample data, the contexts and limitations of these mechanisms, and the outcomes that can be extracted from the sample data.

Step 6: Report status. This step considers a description of how the framework refinement identified or proposed in step 5 compares with the initial theoretical framework that was described in step 1. This is usually done through a two-step process. A descriptive analysis is presented first, followed by a thematic analysis.

- In the descriptive analysis the data is presented according to their numbers and characteristics such as volume, distribution, authorship or source.
- In the thematic analysis the synthesis sample is discussed according to the chosen theoretical framework, and the findings are presented and narrated through descriptions, diagrams and categorizations.

2.6 Descriptive analysis

The descriptive analysis summarizes the documents considered for the synthesis sample according to characteristics regarding the year of publication, academic journal or conference of publication, industries, and applied method. The analysis ends by providing an assessment of the maturity of the field.

Based on the inclusion and exclusion criteria, the process of the literature review resulted in 323 documents. These documents were reviewed according to the exclusion/inclusion criteria and resulted in a final refined document list, i.e., the synthesis sample, based on which the analysis was performed. The overall process is shown in Figure 7.

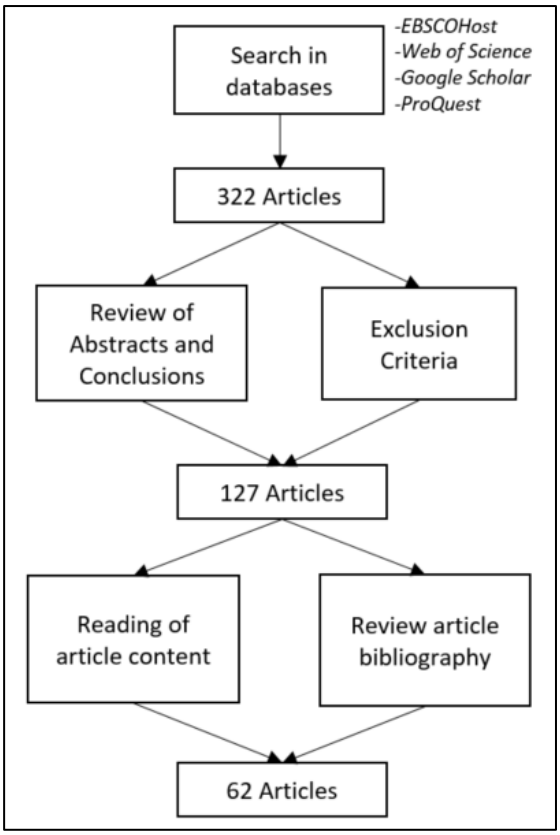

Figure 7 Review process for the sample selection

The synthesis sample consisted of 62 documents ranging from the year 2000 to 2017, with over 80% of the documents in the synthesis sample being peer-reviewed journal articles, as shown in Figure 8. A complete list of the papers considered in the synthesis sample ordered by year of publication can be found in the Appendix 11.7.

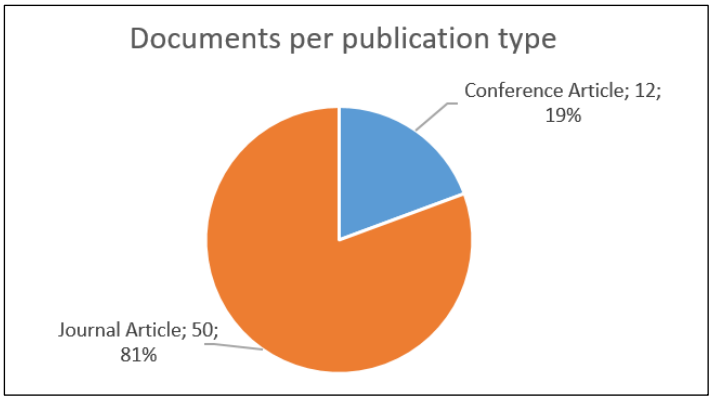

Figure 8 Distribution of documents in synthesis sample

The publication of articles about supply chain cyber-resilience has increased through the years, as reflected in Figure 9.

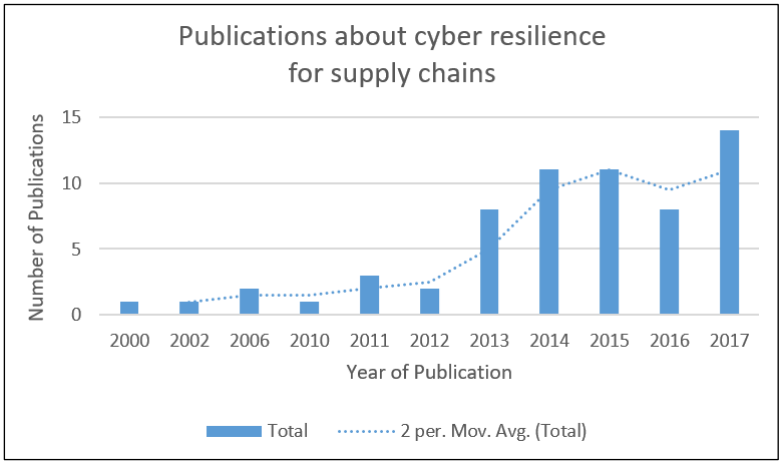

Figure 9 Publications in synthesis sample per year of publication

Table 5 shows the distribution of journals for publications about supply chain cyber-resilience. Four journals provide four or more articles about cyber-resilience with a relevance to supply chains. A deeper analysis shows that these have been special

issues about cyber-resilience or cyber-security, particularly the following journal publications:

- *Environment Systems and Decisions*, volume 33, issue 4, December 2013, a special issue of cybersecurity, risk and decisions, edited by Zachary A. Collier, with 5 articles in the synthesis sample.
- *Journal of business continuity & emergency planning*, volume 7, issue 2, fall 2013, special issue of cybersecurity, edited by Frederick Hult, with 5 articles in the synthesis sample,
- *Technovation*, volume 34, issue 7, July 2014, special issue on security in the cyber supply chain, with 4 articles in the synthesis sample,
- *Technology Innovation Management Review*, volume 5, issue 4, April 2015, special issue about cyber-resilience in supply chains, edited by Omera Khan and Chris McPhee, with 5 articles in the synthesis sample.

Table 5 Journal publications in synthesis sample

Journal Name	**# of publications**
Environment Systems and Decisions	5
Technology Innovation Management Review	5
Journal of business continuity & emergency planning	5
Technovation	4
Proceedings of the IEEE	3
Computers & Security	2
International Journal of Critical Infrastructure Protection	2
International Journal of Physical Distribution & Logistics Management	2
Network Security	1
Computer	1
Politics	1
International Journal of Interactive Multimedia & Artificial Intelligence	1
International Journal of Computer Networks & Communications	1
Quality of Protection	1
Pervasive and Mobile Computing	1
Renewable and Sustainable Energy Reviews	1
International Journal of Computer, Electrical, Automation, Control and Information Engineering	1
Supply Chain Management: An International Journal	1
Information & Security	1
Risk analysis	1
International Journal of Research in Engineering and Applied Sciences	1
Computer Science Review	1
Production Engineering	1
The Electricity Journal	1
Electronics	1
MITRE Report	1
IEEE Transactions on Smart Grid	1
Journal of Cyber Policy	1
Business Information Review	1

Journal Name	# of publications
Journal of Water Resources Planning and Management	1
Grand Total	**50**

The low number of publications over the years and the dispersion of the papers across different journals seem to point towards this being an immature research field. An analysis of the applied research method in the synthesis sample shows over 45% of the articles are descriptive without using specific case examples as shown in Figure 10. Furthermore, the articles do not address an industry or address the industry in a generic form, as shown in

Table 6. This general way of addressing case examples and the industries involved further indicate how supply chain cyber-resilience is an immature field.

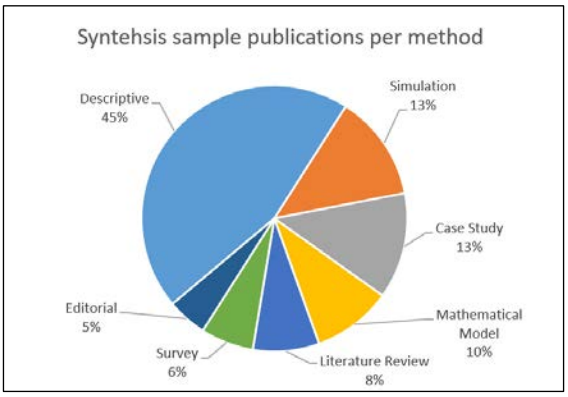

Figure 10 Synthesis sample publications per method

Table 6 Publications in synthesis sample per industry

Industry	**# of publications**
None	17
Generic	9
Critical infrastructures - electric	7
Control systems	5
Government	4
Military	2
Production	2
Critical infrastructures - generic	2
Critical infrastructure - water systems	2
Standards	2
Insurance	2
Maritime	2
Education/training	1
Various (transport /pharma /maritime)	1
Various (oil/production)	1
Engineering development	1
3D printing	1
IT/software/hardware	1
Grand Total	**62**

Table 7 provides an overview of the main conferences where the conference articles in the synthesis sample were published.

Table 7 Conference publications in synthesis sample

Conference Name	**# of publications**
Technologies for Homeland Security (HST)	2
Proceedings of the 2015 Workshop on Automated Decision Making for Active Cyber Defense	2
Resilient Control Systems (ISRCS)	1
Dependable Systems and Networks Workshop	1
Systems and Information Engineering Design Symposium (SIEDS)	1
ICMLG2017 5th International Conference on Management Leadership and Governance	1
Internet of things (iThings/CPSCom)	1
Intelligence and Security Informatics Conference (EISIC)	1
Decision and Control and European Control Conference (CDC-ECC)	1
Nordic Conference on Secure IT Systems	1

The dispersion of conference papers dispersion together with the low number of conferences papers included in the synthesis sample support the claim that the field of supply chain cyber-resilience for the supply chain is an immature field of research.

2.7 Thematic analysis

This section describes, categorizes and discusses the articles in the synthesis sample according to the chosen framework of analysis or "themes", looking to answer the research questions that motivated the SLR. As indicated in section 2.4, the chosen framework of analysis is systems thinking, along three main areas: leverage, feedback and aggregation level. The leverage considers

the identification of the constituent parts of each framework, their relationships, and categorizing according to behaviours, patterns or structures. The Feedback deals with the circular causality structures and thus the dynamics, i.e., variation over time, present in each of the frameworks. Finally, the Aggregation refers to the level at which the framework is grouped, e.g., at a company level, and industrial level or government level, as well as with the type of data that these frameworks require.

The aim of this analysis is to provide a list of comparable descriptions of the literature in the synthesis sample research to answer the research questions that guide the SLR. These questions are:

> *Research sub-question 1 (RSQ1):*
> *What are the supply chain cyber-resilience frameworks published in literature?*

> *Research sub-question 2 (RSQ2):*
> *Which case studies have been published about supply chain cyber-resilience with operational disruption?*

Both of these questions are directed towards answering the main research question:

> *Main Research Question (RQ): How can global supply chains manage cyber-risks and security?*

When comparing the answers that can be obtained from the synthesis sample analysis to the research sub-questions, these answers reveal gaps in the knowledge required to answer the main research question. The gap analysis is described in the last part of the Literature Review chapter, in section 2.9.

The synthesis sample presented a distribution of papers from the three knowledge domains mentioned in section 1.2., namely SCM, R&RM, and ITM. The distribution of the articles is shown in Figure 11. The synthesis sample contained a similar number of papers from SCM and ITM.

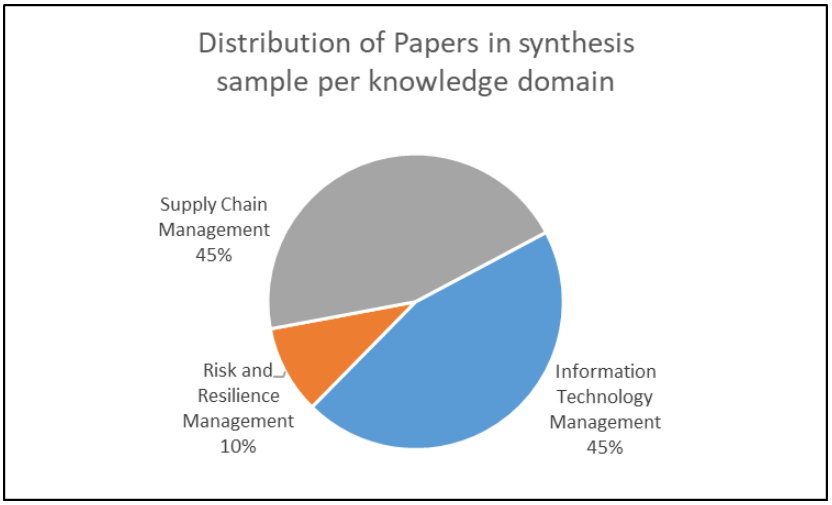

Figure 11 Sample per knowledge domain

The knowledge domain from which the papers originate conditions the approach through which cyber-resilience is presented.

2.7.1 What is cyber-resilience

The SLR revealed a number of definitions for cyber-resilience as shown in Table 8. The earliest definition of cyber-resilience found in the published literature is a definition by Hult et al., from 2014. This is two years later than the earliest reference to cyber-resilience found in other extended literature, in this case, a document by the World Economic Forum from 2012.

The different definitions of cyber-resilience that were found consider cyber-resilience as either an ability (WEF, 2012; Ahmad et al., 2015; Björck et al., 2015; Davis, 2015; Khan et al., 2015b;

Arghandeh et al., 2016), a capability or capacity (Hult et al., 2014; Khan et al., 2015a).

Table 8 Cyber-resilience definitions in the synthesis sample

Cyber-resilience definition	**Reference**
Cyber-resilience is the ability of systems and organizations to withstand cyber events, measured by the combination of mean time to failure and mean time to recovery.	WEF, 2012
Cyber-resilience is the capacity of an organization to remain healthy in an environment of permanent conflict and constantly evolving cyber attacks	Hult et al., 2014
Cyber-resilience refers to the ability to continuously deliver the intended outcome despite adverse cyber events by humans and nature.	Björck et al., 2015
Cyber-resilience is the ability to anticipate, withstand, recover from, and evolve to better address cyber threats	Ahmad et al., 2015
Cyber-resilience is the ability of a system that is dependent on cyberspace in some	Davis, 2015

Cyber-resilience definition	Reference
manner, to return to its original or desired state after being disturbed.	
Cyber-resilience is the capability of a supply chain to maintain its operational performance when faced with a cyber-risk	Khan et al., 2015a
Cyber-resilience is the ability of a system to resist against or minimize, the potential damage in order to maintain the system state within an accepted operational level in response to an external cyber threat or cyber-attack.	Khan et al., 2015b
Cyber-resilience is a system's ability to reduce the magnitude and duration of a disruption when faced with an unexpected set of disturbances, by altering its structure in an agile way.	Arghandeh et al., 2016

Ability is defined as a natural aptitude towards doing something, and the capability as the potential of a system towards doing something (Merriam-Webster, 2017).

While ability points to what a system is currently in a position to do, capability points towards what a system could end up doing, or the extent to which its ability may reach. As an example, a person that has the ability to play the piano also has the capability of playing Rachmaninov's 3rd piano concerto. This particular person's ability to play the piano could thus extend to accomplishing a piano concerto.

Given the unexpected (Arghandeh et al., 2016) or constantly evolving (Hult et al., 2014) characteristics of the cyber-risk-derived disruptions that lead to the manifestation of cyber-resilience, it would be better described as a capability. Therefore this thesis considers cyber-resilience as:

"The capability of a system to minimize the effects on expected performance of a disruption caused by the manifestation of a cyber-risk"

With this definition, cyber-resilience is considered a capability as it is the extent to which the current combination of abilities can help to obtain the desired outcome, i.e., maintaining the expected performance. Additionally, both external and internal sources of cyber-risk and both intentional and unintentional sources of disruption are also considered in the definition.

2.7.2 Level of aggregation for cyber-resilience

The Aggregation level explores the way in which the information about cyber-resilience is grouped, and the type of information that would be required to apply the framework.

The synthesis sample revealed papers with different levels of aggregation. Figure 12 shows the distribution of papers for three levels of aggregation, government level, industry level, and company level.

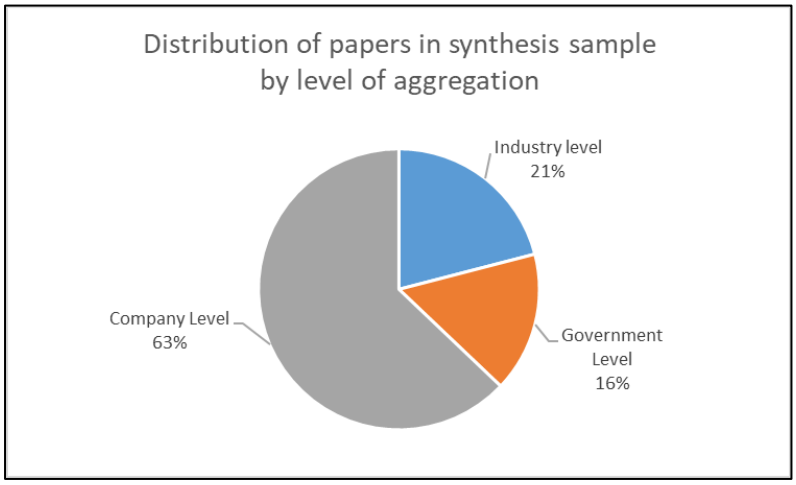

Figure 12 Aggregation for papers in the synthesis sample.

63% of the papers in the synthesis sample consider cyber-resilience at the company level, while government level and industry level articles share similar proportions of the total, 16% and 21% respectively. However, only a few of the articles address the problem of the aggregation level for cyber-resilience analysis.

Björck et al., (2015) presented a number of levels of aggregation for understanding cyber-resilience, which have been grouped within the government, industry and company levels:

- Government level:
  - Supranational level, i.e., an aggrupation of nations, e.g., the European Union,
  - National level, i.e., a particular country or society, e.g., Denmark,
- Industry level
  - Regional level, i.e., a particular region or city, e.g., the great Copenhagen region,
- Company level
  - Organizational level, i.e., a specific organization or company, e.g., the Technical University of Denmark, DTU,
  - Functional level, i.e., a specific business function, e.g., the supply function in an organization,
  - Technical level, i.e., a specific technical system, e.g., the control systems present in the purchasing function

Björck also argues that "*these levels have to be addressed in parallel for cyber-resilience to be effective*" (Björck et al., 2015).

An analysis of the knowledge domains of the articles in the synthesis sample shows a clear relationship: as can be seen in Figure 13, the articles from the SCM domain are chiefly

government or industry level analyses, while the IT domain papers chiefly correspond to company level analyses.

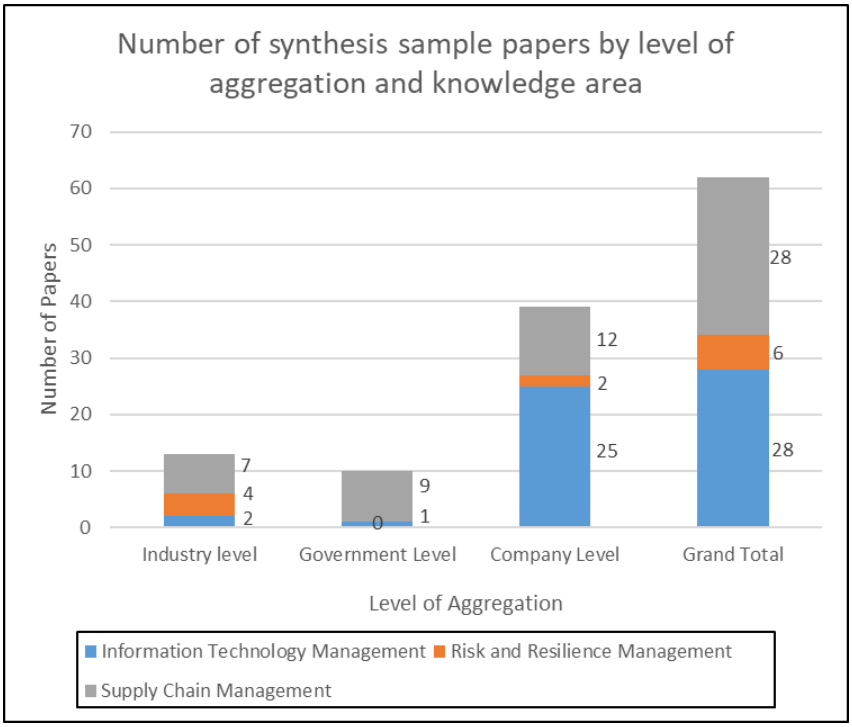

Figure 13 Aggregation and knowledge domain in sample

2.7.3 Cyber-resilience versus cybersecurity

The SLR revealed different authors describing cyber-resilience as having evolved from cybersecurity. At the same time, there is mention of insufficient clarity on how these two concepts differ, and how this can lead to problems (Zhu et al., 2011; de Crespigny, 2012; Fink et al., 2014; Hult et al., 2014; Ferdinand, 2015; Arghandeh et al., 2016; Conklin et al., 2017; Jin et al, 2017).

Cybersecurity has been described as being mostly concerned with attacks coming from outside the organization, of establishing perimeter defences in a castle mentality (Hult et al, 2014), with a focus towards maintaining IT infrastructure availability and of giving the right people access to resources. Additionally, both IT and cybersecurity have also been characterized as slow in adapting to malicious activity from insider sources (Hult et al., 2014).

As illustrated in Figure 14, to characterize the main objectives of IT and cybersecurity, a triad for IT-security has been proposed consisting of confidentiality, integrity, and availability of data and communications known as the "*CIA triad*" (Goldman, 2010; Zhu et al., 2011; Boyes, 2015; Li et al., 2017).

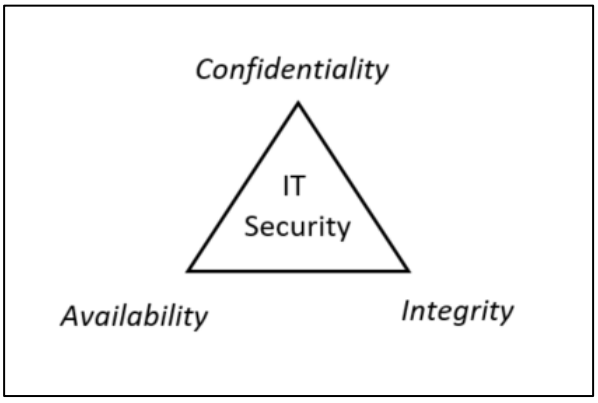

Figure 14 CIA triad of IT Security (based on Zhu et al., 2011)

It is important to note that despite similarities, IT security and cybersecurity are not strictly synonyms. IT security is a broader concept as it considers the protection of data in whichever format

this data is stored and communicated in the organization. Cybersecurity deals with the protection of data in electronic format, and it also deals with the protection required as a result of the network connectivity achieved by the Internet.

Given that since cyber-risks focuses on data in electronic format, IT security and cybersecurity for the ends of this thesis, despite being terms not strictly synonymous, should be nevertheless considered as equivalent. A similar consideration should be had with the terms IT-Infrastructure and cyber-infrastructure.

The synthesis sample described cyber-resilience as 1) multidisciplinary and requiring integration across departments (Hult et al., 2014), 2) driven by organizational learning and capabilities, i.e., being able to change quickly defence and investment strategies as a reaction to cyber-attacks, thus requiring a dynamic capability process (Ferdinand et al., 2015), 3) being insightful towards the adversary and intelligence-driven, and 4) part of the values of the organization instead of merely a set of procedures (Hult et al., 2014).

These differences can be summarized for each of the two concepts of cyber-security and cyber-resilience according to 1) aspects of behaviour, e.g., objective and aim, 2) aspects of pattern e.g., the approach considered for each of the two concepts, and 3) aspects of structure, e.g., the architecture and scope of each

concept. A comparison of these dimensions is described in Table 9.

Table 9 Cybersecurity versus cyber-resilience

	Cybersecurity	**Cyber-resilience**
Objective	Protect IT Systems (Björck et al., 2015, Zhu et al., 2011)	Maintain business delivery performance (Björck et al., 2015)
Aim	Fail-Safe (Björck et al., 2015) Must identify and prepare for all cyber-attack cases (Ferdinand, 2015)	Safe-to-Fail (Björck et al., 2015) Defence against all possible cyber-attacks is unrealistic (Goldman, 2010; Ferdinand, 2015) Complete mission despite cyber-attacks (Goldman, 2010)
Approach	Apply security from outside (Björck et al., 2015) Building perimeter protection (Hult et al., 2014) Top-down control mechanism in static environment (Boyson, 2014)	Build security from within (Björck et al., 2015) Capability-built reaction (Hult et al., 2014) Address fundamental mechanisms and real-time world scale of adaptive IT Networks (Boyson, 2014) Re-architecting of systems for resilience (Goldman, 2010)
Architecture	Single-layered protection (Björck et al., 2015)	Multi-disciplinary and integrated across departments and disciplines (Hult et al., 2014)

	Cybersecurity	**Cyber-resilience**
	Information and embedded automation systems are the key protected assets (Hult et al., 2014) Purely technical means of control (Boyson, 2014)	Multi-layered protection (Björck et al., 2015) Managerial and human factors engineering in preventing risks from disrupting IT system's operations (Boyson, 2014) High level of collaboration, information sharing, cross-training and influencing
Scope	Atomistic, one organization (Björck et al., 2015)	Holistic, network of organizations (Björck et al., 2015) Cybersecurity as part of the organization's values (Hult et al., 2014) Requires structural integration (Boyson, 2014)

2.7.4 Cyber-resilience frameworks

Very few of the resilience frameworks present in the synthesis sample are described as derived, i.e., are incremental contributions, from other previously proposed resilience works. As Figure 15 shows, more than 90% of the papers in the synthesis sample did not make reference to any other resilience framework. Moreover, as shown in Table 10, over half of the papers in the

sample, i.e., 33 papers or 53% of the total, made a descriptive analysis of the cyber-resilience problem and 26 out of the total 62 articles (42% of the total) proposed a framework starting from an original analysis independent of any existing resilience framework, in what could be called a fundamental analysis.

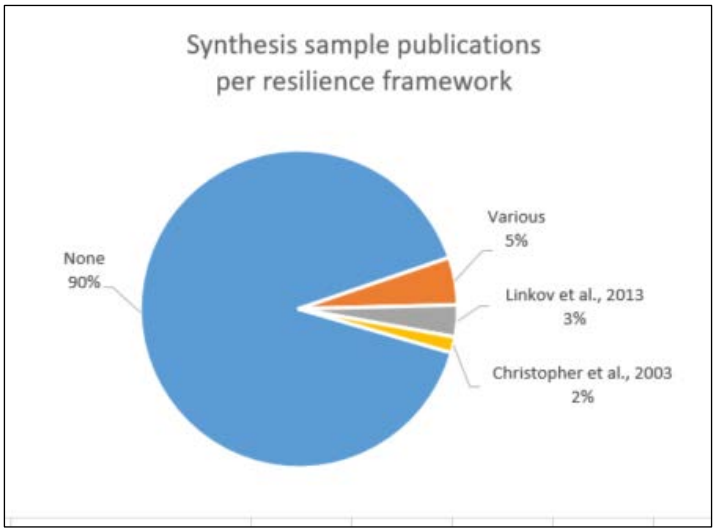

Figure 15 Sample publications per resilience framework

The term "*fundamental analysis*" is used mainly in investment theory. It is, however, a term with a broader implication, and it means an analysis starting from the fundamental forces that create the phenomenon that is being described. In the sense of cyber-resilience frameworks, a fundamental analysis starts from assumptions about the reality being described, towards the proposal of equations or models based on those assumptions.

Table 10 Papers in synthesis sample per resilience framework

	Presents Framework		
Resilience Framework	**Yes**	**No**	**Total**
Christopher et al., 2003	1	0	1
Linkov et al., 2013	2	0	2
None	26	30	56
Various	0	3	3
Grand Total	**29**	**33**	**62**

The earliest reference to cyber-resilience is the management of disruptions derived from cyber threats to the supply chain by Warren et al., (2000), where a general framework of managerial interventions to counteract cyber-risks was described. Three types of interventions were defined: 1) technical interventions to the supply system, 2) formal interventions to improve organizational and official hierarchical aspects of the supply system, and 3) informal interventions, which would be directed to improving the human aspects of the supply system.

This general categorization of intervention types reflects one of the characteristics of supply systems, namely the co-existence of different dimensions of activity. The proposal by Warren et al. (2000) is general and does not specify what these "*human*" aspects consider or what form these "*interventions*" should take. Warren et al. (2000) do not consider any evolution over time hence it is a static analysis.

A static analysis does not consider time as a factor, and it is descriptive of a specific state of a system at some point in time. In contrast, a dynamic analysis considers time, and more specifically the change of the system state through time, as the relevant point of description and analysis.

The proposal by Warren et al. (2000) does not venture into the organizational structures that are necessary, and focuses on the patterns to be avoided, i.e., risk types, and the patterns to be followed to minimize these risks, i.e., intervention types. The analysis is presented at a company level and with a strategic outlook, presenting overall aims of cyber-resilience.

Williams et al. (2002) proposed the notion of "*electronic supply chain*" or "*eSC*" considering variation over time as a relevant aspect of analysis, identifying as an advantage that "*eSC are dynamic and adaptable*" (Williams et al., 2002).

Thus, these authors described the use of electronic supply chains as suitable for vertical integration, allowing for relationships in the supply chain to move from being merely competitive to collaborative. This move changes the paradigm from a cost-based to a value-based relationship formation.

The management of electronic supply chains is proposed by Williams et al. (2002) as a circular, nested process with the focal company at the centre, and the different stakeholders with whom a connection is made "*as long as a need is met*", and thus changing

over time. Due to the dynamic character of the required stakeholder connections, Williams et al. (2002) highlight an important advantage of electronic supply chains as the ability to reconnect or disconnect as necessary, with high speed and lower transaction costs than what they call traditional “arms-length” stakeholder relationships.

The description by Williams et al. (2002) is strategic and at the company level. They take a dynamic approach to understanding the management of electronic supply chains. This approach is presented as a circular, recurring process that adapts over time and is as such “*extremely dynamic*”.

The description by Williams et al. (2002) proposed advantages of electronic supply chains that have not completely materialized. The connectivity architecture does not consider the practice to connect and disconnect from supply chain partners constantly, but rather have a constant connection that is used as necessary.

Both Williams et al. (2002) and Warren et al. (2000) mention the electronic supply chain as a different challenge with respect to the existing traditional supply chains. However, despite outlining the types of advantages and risks that result from using an electronic supply chain, they do not provide an actionable framework through which to manage the reaction of the supply chain when the risks materialize.

Goldman (2010) explored the architecture of what is a resilient system. Architecture is "*the way in which a system is purposefully built for a certain objective aesthetic and functional*" (Merriam-Webster, 2017), and it considers design, method and implementation. Therefore, Goldman looks at structures that are responsible for the cyber resilient behaviour that is required.

Goldman proposes looking at the structure instead of only protection since "*the notion that we can achieve 100% protection is not only unrealistic but also results in a false sense of security*" (Goldman, 2010). Furthermore, "*we must change our current philosophy that we can keep adversaries out or detect their breaches with our first-line defences*".

Goldman, therefore, argues resilience and particularly cyber-resilience should be built on the concept of survivability, combining the disciplines of performance, security, reliability, fault tolerance, and safety to "*support a balanced combination of protections, detections and adaptive technical and operational responses that respond dynamically*" (Goldman, 2010). For this end he proposes a cycle of objectives, 1) protect and deter, 2) detects and monitor, 3) constrain and isolate, 4) maintain and recover, and 5) adapt.

Protect and deter is a result of the adaptive objectives, represented through the implementation of the best security practices, the assurance of hardware and software integrity and

correctness, the protection of the data, the minimization of the essential functions of the system, the consideration of data replication, redundancy and diversity, the tolerance of some level of failure, and the development of offensive ability.

Detect and monitor is a result of the protection and deterrence objectives, represented through the detection of anomalous symptoms both in own system and in the connected partners, the monitoring of operating conditions, and the collection of data for forensic analysis.

Constrain and isolate is a result of the detection and monitoring objectives, represented through the capacity to configure continuity of operations and disaster recovery, and the integration of safeguards to contain spread and propagation of damage.

Maintain and Recover is a result of the constraints and isolation objectives, represented through the capacity to degrade parts of the system when necessary, the capacity to "*fail in a good way*" (Goldman, 2010) when necessary, and the capacity to return to the required operating conditions.

Adapt is a result of the maintenance and recovery objectives, represented through the capacity to operate adaptively, the capacity of use hardware, software, data, and processing diversity in random ways, the capacity to return quickly to acceptable levels of trust, and the ability to confuse the adversary by introducing unpredictability, deception and randomness.

This dynamic framework proposal is shown in Figure 16 (Goldman, 2010).

Figure 16 Resilient architecture cycle (Goldman, 2010)

Goldman (2010), introduces several relevant aspects 1) a dynamic approach towards the resilient architecture, 2) the fault tolerance approach to consider recovery of operations as a central feature of resilience beyond prevention and 3) the indication of trust as a relevant feature for recovery as part of the adaptation process. Another relevant contribution is that his approach does not start with the analysis of the cyber-attacks themselves, i.e., the traditional ways of protection, but instead from the analysis of the architecture of the system that is vulnerable to these cyber-attacks.

Goldman does not propose any quantification to these mechanisms and the proposal at the company level of aggregation.

A common theme among the papers in the synthesis sample is the "*situational awareness*" required to obtain information to make decisions. Four domains have been identified by Collier et al., (2013), namely the physical, information, cognitive and social domains. Initially identified for IT security, Linkov et al., (2013b) extended their use as part of his resilience framework for cyber-systems, from an original application to a generic resilience framework (Linkov et al., 2013a).

The framework as proposed by Linkov et al., (2013a), is the earliest evidence of an explicit, actionable framework to evaluate the resilience of cyber systems. In this framework Linkov et al (2013b) combine two independent dimensions for the assessment of a cyber-system: 1) the four domains as mentioned by Collier et al., (2013), and 2) the phases of an "event management cycle, namely plan/prepare, absorb, recover, and adapt, as proposed by the National Academy of Sciences (Cutter et al., 2013). This matrix is shown in Figure 17.

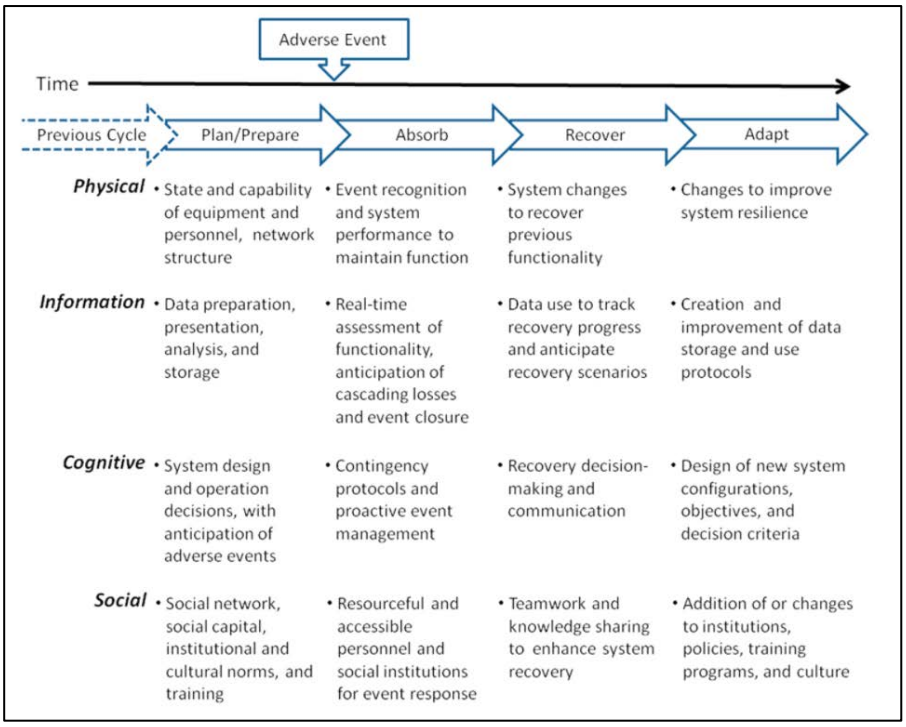

Figure 17 Resilience matrix (Linkov et al., 2013a)

Right from the outset of his first proposal for this matrix resilience framework, Linkov et al. (2013a) have argued for two important obstacles for measuring and thus managing resilience.

First, the relative success of quantitative risk assessment as a dominant paradigm for the design and management of systems means that "*the pervasive concepts of risk have encroached upon the understanding of resilience*" (Linkov et al., 2013a). This creates a difficulty in understanding the concept of resilience in general and cyber-resilience in particular, as these are concepts with a much broader scope than risk and cyber-risk respectively,

and are "*essential when risk is incomputable*" (Linkov et al., 2013a).

Second, Linkov et al., argue that the fragmentation of the knowledge about resilience allows only for incremental improvements towards known risks, while critical infrastructure cyber-resilience "*requires a generalizable approach that is both applicable to a diverse array of systems and is revealing of their interconnectivity*" (Linkov et al., 2013).

According to Linkov, the areas where relevant resilience knowledge for cyber systems is fragmented include environmental management, engineering infrastructure, and cybersecurity.

Overall, 44 of the 62 articles in the synthesis sample (71%) did not mention change over time in their description and have thus been considered as static assessments. Of the articles that actually proposed some sort of model for cyber-resilience (29 articles), 52% of them (15 articles) did not mention change over time as a relevant factor.

2.7.5 Cyber-risks in supply chains

Warren et al., (2000) mention the risks that are associated with a supply network and which are derived from IT-dependent processes: 1) the theft of passwords, 2) fraudulent communications, 3) traffic overloading, and 4) direct attack.

Methods for *password theft* include systematically using possible password combinations until one works out, i.e., cracking, or remotely recording the password when entered by an approved user, i.e., sniffing. Successfully stolen passwords can then be used to access content restricted to the original password owner.

Fraudulent communication is produced by transmitting messages that appear to be legitimate or by faking information about the origin of the message, allowing the acceptance of this message by the receiver. This is called message spoofing. A different type of spoofing was identified as the fraudulent creation of a website that appears to be legitimate, and as a result get unsuspecting users to share some confidential information. This is called web spoofing.

The *purposeful overloading of the digital traffic* is created towards a specific digital destination, to disable its function temporarily. In this way, the availability of these systems is obstructed for legitimate use. An example of this is what Warren et al., (2000) calls the “ping of death”. “Ping” is a type of message sent from one computer to another to find out if the destination computer is active. The destination computer can be affected by sending repeated ping messages and thus disabling its use for other purposes, or a ping message can be sent that is too big

causing the destination machine to crash or reboot. These attacks are called Denial of Service Attacks (DDOS).

Finally, the *direct attacks* identified by Warren et al., (2000) were broadly described as "*hacking to destroy, modify or extract data*", without specifying the detail process to achieve these.

Goldman (2010) explores the techniques and mechanisms for cyber-resilience from the point of view of the particular characteristics of cyber-threats.

The following table shows this relationship between the techniques and their characteristics, with the specific cyber-threat characteristic that Goldman (2010) indicates the technique seeks to address.

Table 11 Cyber threat characteristics vs. cyber-defence techniques

Resilience technique	**Technique characteristics**	**Cyber-threat characteristic**
Diversity / Redundancy	Designed into hardware, software and components.	Single point of contact can have multiple consequences in similar parts of the system, and cause systems to fail sequentially (cascade effects)
Integrity	Beyond integrity checks, e.g., MD5, SHA, validate different independent and random parts of the system	Cyber threats that change existing information, code or function of a system, are often invisible, and render contingency plans such as replication or transfer of services, ineffective.
Isolation / Segmentation / Containment /Least privilege	Separate critical from non-critical data and connections.	Cyber-threats take advantage of connectivity and interconnections
	Separate activities and data for different levels of privilege	Cyber-attacks access through the untrustworthy parts of the system (e.g., end-user client systems)
		Cyber-threats outpace patching, which is reactive.
Detection / Monitoring	Correlation of meaningful threat indicators and trends, and detecting compromises to integrity	Cyber-threats need not immediately have an effect, but merely gather data.
Non-persistence	Image keeping of systems for restoration, Evaluate if continuous connectivity is essential.	Cyber threats affect systems that can be restored to a previous state, and access can be eliminated when necessary

Resilience technique	**Technique characteristics**	**Cyber-threat characteristic**
Distributed and moving target defence	Decentralize processing, distribute data, and synchronize as necessary. Randomize this process.	Single point of contact can have multiple consequences in similar parts of the system, and cause systems to fail sequentially (cascade effects)
Adaptive management and response	Have damage assessment dynamic capability	Cyber-threats create damage which can be unpredictable
Randomness unpredictability and deception	Techniques such as Misinformation, Entrapment techniques (e.g., Honeypots), customized protocols, code, solutions, self-protecting data- self modifying code, code and data *obfuscation.*	Cyber threats gather data and patterns to identify targets

Other authors expand on the taxonomy of cyber-risks from the economic perspective (Min et al., 2005; Andrijcic et al., 2006) and from the human factors perspective (Brown, 2016; Wilding, 2016)

2.7.6 SCADA as cyber-physical interfaces

Several of the papers in the synthesis sample went beyond strategy to explore the way in which cyber-threats affect operations, particularly through SCADA. The Supervisory Control And Data Acquisition (SCADA) systems are systems that use computers, networked data and graphical user interfaces to

manage processes from a high-level. SCADA systems are seen as crucial components of operational systems to gather data for decision making, and are a direct interphase between digital data and the physical consequences of a decision made with that data (McQueen et al., 2006; Zhu et al., 2011a; Onyeji et al., 2014; Barron et al., 2016; Taormina et al., 2017; Ashok et al., 2017; Li et al., 2017).

Despite being used for decades in different forms, SCADA systems remained relatively obscure in the cyber-threat landscape until the news of the most significant cyber-attack against critical infrastructure up until then (Onyeji et al., 2014), the Stuxnet malware attack against the Natanz nuclear-enrichment facility in Iran starting in 2009.

The relevance of SCADA systems can be described through a generalized process control diagram, illustrated in Figure 18.

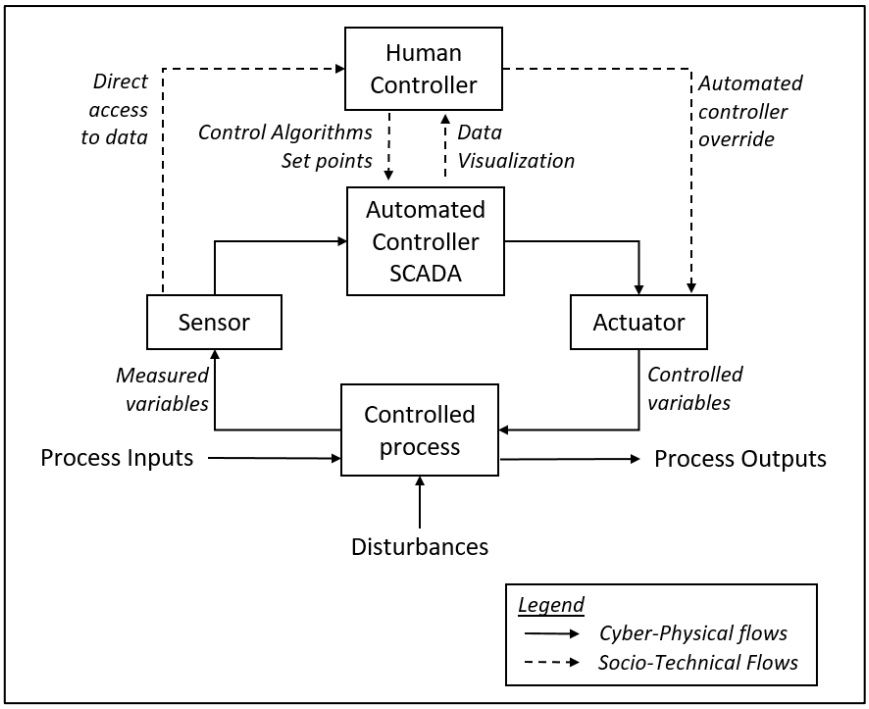

Figure 18 Control process diagram

The SCADA is a central part of the operation as it uses control algorithms defined by human controllers to influence a controlled process in the real world, in a decision loop that adjusts according to the information obtained from sensors about the world. "*Control systems*" are a ubiquitous concept used to experience and interact with the world.

SCADA systems obtain information from the controlled process through sensors, process this information according to some type of algorithm and react by acting on the controlled process through some type of actuator. This is a continuous process of adjustment in a flow that makes the physical world

interact with information that is generated from it, i.e., a cyber-physical system.

Additionally, the decision algorithms are determined by an objective set by a human controller who does not necessarily take an active part in the process control. The human controller is informed by some interface in the SCADA system about the current and historical operating conditions. Furthermore, this human controller can override the SCADA system by directly activating the actuators or by directly obtaining information from the sensors.

SCADA systems differ from other IT systems in their primary security goal: while IT security focuses on the protection of the server over the user, SCADA security focuses on protecting the performance of the process (Zhu et al., 2011), and is thus closer to what is understood as cyber-resilience. SCADA systems were originally intended as closed systems, yet they are being connected to the Internet to drive physical infrastructure, increasing the risk of security breaches (Onyeji et al., 2014). Thus, SCADA systems are increasingly the subject of case analyses to identify the taxonomy of the cyber-risks to which they are exposed (Zhu et al., 2011). Moreover, simulations have been recently used to understand SCADA systems reactions to prospective attack scenarios (Taormina et al., 2017).

2.8 Answering the initial research sub-questions

This section details the answers to the research sub-questions that justified the SLR. It discusses 1) the extent of the answers that are possible with the evidence that was obtained from the synthesis sample and 2) the aspects which are not possible to answer with the data that that was obtained, i.e., gaps in the knowledge. These gaps result in further research questions pursued during the remaining thesis.

2.8.1 Research sub-question 1

The first research sub-question relates to the existence of frameworks for managing cyber-resilience in supply chains:

> *Research sub-question 1 (RSQ1):*
> *What are the supply chain cyber-resilience frameworks published in literature?*

According to the systems thinking framework level involved, the cyber-resilience frameworks found from the synthesis sample were catalogued either as descriptive, normative or quantitative. Descriptive frameworks concentrate on the events, normative frameworks focus on the patterns behind events, and the quantitative frameworks delve into the structures that generate those patterns.

The descriptive frameworks were the frameworks found in the older data, are mostly derived from the SCM knowledge domain, and are primarily strategic in nature. The identified descriptive frameworks that were found provided organizational, macroeconomic or systems descriptions of the cyber-resilience phenomenon.

72% of the identified frameworks in the synthesis sample are normative frameworks that deal with the patterns underlying cyber-resilience. The sample presented an even distribution between frameworks from the SCM and the ITM knowledge domains. Moreover, there was an even distribution between strategic and operational approaches.

The quantitative frameworks were found to be more recent and derive from the ITM knowledge domain. These frameworks are mostly operative in their approach. The frameworks and their descriptors - knowledge domain, and strategic versus operative - is laid out in Table 12.

Table 12 Cyber-resilience frameworks found in the literature

Type	Description	Supporting Literature	Strategic	Operative	SCM	ITM	R&RM
Descriptive (Event Related)	Focal Company with concentric stakeholders	Williams et al., 2002	x		x		
	Macroeconomic descriptive evaluation	Andrijcic et al., 2006; Kelic et al., 2013;	x				x
	Systems description	DiMase et al., 2015	x		x		
Normative (Pattern Related)	Resilient Architecture	Goldman, 2010; Goldman et al., 2011; Lee et al., 2017; Conklin et al., 2017	x			x	
	Robust and Resilient Control	Zhu et al., 2011; Krotofil et al., 2013; Arghandeh et al., 2016; Li et al., 2017		x		x	
	Four Domains of Cyber resilience	Collier et al., 2013	x		x		
	Plan/prepare - absorb - recover - adapt cycle	Linkov e al., 2013	x		x		
	Autonomous reconstitution	Ramuhalli et al., 2013		x		x	
	Attack graphs	Abraham et al., 2015		x		x	
	Multi-network	Choudhury et al., 2015; Taormina et al., 2017		x		x	

Type	Description	Supporting Literature	Strategic	Operative	SCM	ITM	R&RM
	Information-centric approach	Davis, 2015	x		x		
	Monitor - analyse - decide - change cycle	Ferdinand et al., 2015	x		x		
	5-layer networked architecture	Harrison et al., 2016		x		x	
	Wide area monitoring, protection and control (WAMPAC)	Ashok et al., 2017		x		x	
Quantitative (Structure Related	Time to Compromise	McQueen et al., 2006	x			x	
	Resource exhaustion cyber resilience	Fink et al., 2014		x		x	
	System Dynamics simulation of cyber resilience (Epidemiological)	Tran et al., 2016	x				x

2.8.2 Research sub-question 2

The second sub-question refers to the experience gathered about the cyber-attacks on supply chains.

Research sub-question 2 (RSQ2):
Which case studies have been published about supply chain cyber-

resilience with operational disruption?

From the synthesis sample, only 6 of the papers (10%) presented case descriptions of cyber-attacks. Most of the papers (80%) that presented a case were from the SCM knowledge domain.

Table 13 Cases presented in the synthesis sample papers

Case industry	Paper year	Case year	Supporting literature	Anonymous?
Education/Training	2012	Future Project	Rajamäki et al., 2012	No
Nuclear	2013	2010	Herrington et al., 2013	No
Pharmaceutical Industry	2014	2010	Boyson, 2014	Yes
Government Agency	2014	2011	Boyson, 2014	Yes
Communication systems	2015	1998	Ahmad et al., 2015	No
Maritime industry	2015	2011	Jansen, 2015	No
Retail industry	2015	2012	DiMase et al., 2015	No
Entertainment Industry	2015	2014	DiMase et al., 2015	No
Communication Systems	2016	2001	Tran et al., 2016	No

Beyond the presentation itself, the way in which the cases are presented is also relevant. Only the cases for the nuclear industry (Herrington et al., 2013), and the communication systems cases (Ahmad et al., 2015; Tran et al., 2016) contain some type of

structure of action through which a cyber-attack became an operational disruption.

2.9 Expanding the research questions

Having provided answers to the research sub-questions 1 and 2, the next step consists of confirming if these answers are sufficient to answer the main research question, and if not, where the gaps lie. These gaps then structure the subsequent questions that are to be further answered by this thesis.

Answering the main research question seeks to provide ways in which cyber-risks can be managed in the global supply chain:

> *Main Research Question (RQ): How can global supply chains manage security from, and resilience to cyber-risks?*

A definition of management is "*the judicious use of means to accomplishing an end, through conducting or supervising something*" (Merriam-Webster, 2017). From the answers that are provided to the research sub-questions, 1 and 2 different gaps can be identified. The gaps that have been classified as either referring to 1) the cyber-risks being managed, 2) the methods that have so far been proposed to manage the phenomenon of cyber-risk and

resilience in the supply chain, or 3) the people using the proposed methods to manage the phenomenon of cyber-risk and resilience in the global supply chain. Each gap type is discussed in detail.

2.9.1 Gap type 1: the reporting of cyber-risks

The synthesis sample shows that there is a clear lack of evidence in the published literature about the cyber-disruptions. This is reflected by the low number of cases that were described in the papers of the synthesis sample. Despite this SLR having been a comprehensive search of published literature, this lack of case evidence is not necessarily surprising due to factors such as the long reporting cycles, unreliable reporting and underreporting.

Long reporting cycles. As indicated in Table 13, the average time from the point when the cases were experienced until when these were published is 6,2 years. This is an exceedingly long time for events of cyber-attacks that have been unfolding rapidly. For example, the Wannacry virus attack event that was mentioned during the introduction made use of an exploit[1] which had been made public by the website Wikileaks only two months previously. With examples of two-month implementation cycles

[1] Exploit is understood in this context as a software tool designed to take advantage of a flaw in a computer system, typically for malicious purposes.

by hackers, reporting cycles of over 6 years severely question the suitability of the peer-reviewed process as it currently stands, for understanding and advancing the science around cyber-risks and security in supply chains.

Unreliable reporting. Onyeji et al., (2014) indicate that "*exact global figures on cybercrime are difficult to locate and prone to inflation*", and the phenomenon suffers a general lack of reliable data (McQueen et al., 2006). In a revealing article, Florencio and his team argue for the unreliability of the available information about cyber-crimes, as research shows that cyber-crime estimates "*appear to be largely the answers of a handful of non-representative people extrapolated to the whole population*", with "*vagueness and lack of clarity about what is being measured*" and that "*75% of the cyber-crime estimates come from unverified self-reported answers*" (Florencio et al., 2013). Hyman (2013) argues that the reports about the effects of malware should not be created by companies that profit from the commercialization of anti-malware software as this would lead to inflated statistics to scare consumers into purchasing their products. Similarly, Herrington et al., (2013) argue that "*most cyber-crime statistics are contested*", by being perceived as "*merely a sales promotion exercise for specialist security firms*". Moreover, official agencies have been severely criticized in the calculation of the cost of cyber-crime, for the lack of transparency in ascribing probabilities to the occurrence of cyber-attacks, based on "*questionable*

calculations that are impossible for outsiders to verify" (Moore, 2011), revealing a problem of transparency in the process of cyber-risk calculation. Onyeji et al (2014) also mention that "*determining the likelihood and severity of cyber-risks have proven to be very difficult*". These phenomena would add to the unreliability of the available information about cyber-crime.

Underreporting of incidents. Different authors report the high likelihood of underreporting of cyber-crimes (Hyman, 2013; Herrington et al, 2013; Onyeji et al., 2014). Hyman (2013) indicates four hurdles that seem to be driving a generalized underreporting of cyber-events. 1) market incentives not to report due to effects on the business performance of the reporting companies, such as the reticence of many organizations about reporting of cyber-crimes to government agencies because they do not trust how the information is used 2) a self-selection bias derived from the losses, i.e., the higher the perceived loss from a cyber-crime, the more likely the company is to report it, and the likelihood of companies with small or no perceived losses to avoid reporting the cyber-crime, 3) the lack of a standard mechanism for reporting cyber-crimes, with no widespread method for including the costs of cyber-crime. For example, Hyman (2013) mentions downtime costs, cost of buying new equipment or the cost of upgrading the security as being included at times in the losses from cyber-crimes, 4) undetected losses, as many organizations are not aware of the losses they have had from an undetected

cyber-crime. Similarly, Herrington et al., (2013) mention that "*victims are not ready to admit to cyber-breaches, and in some cases, they do not know that they have been attacked*". An example of this is a cyber-attack to the port of Antwerp in 2013; when it was discovered, it was at least 2 years old (Boyes, 2015).

Of the cases that were reported, 60% of them made reference to the economic implications of the cyber-crimes, and only 30% of them made any reference to the way in which these cyber-crimes actually created the disruption. Therefore, the data gathered through the SLR gives evidence of a lack of information about how the cyber-crimes actually result in operational disruptions affecting business, due to insufficient information on the mechanisms that result in the disruption.

2.9.2 Gap type 2: the methods being used

With respect to the methods that have so far been proposed to manage the phenomenon of cyber-risk and security in the global supply chain, two main gaps were found in the literature that was reviewed through the SLR, related to the compartmentalization of the knowledge about cyber-resilience, to the static nature of current frameworks, the historical-dependence of current methods, and the suitability of current methods for managing cyber-risks.

Compartmentalization is "*the separation into isolated categories or compartments*" (Merriam-Webster, 2017). Compartmentalization in the understanding and management of cyber-risks was mentioned by different authors as either a need for a more comprehensive method; (Khan et al., 2015b), or a calling for structural integration (Boyson, 2014), through approaches such as addressing jointly multiple levels of aggregation through which cyber-resilience can be understood (Björck et al., 2015), or addressing the different domains where cyber-resilience decision making takes place, namely the physical, information, cognitive, and social domains (Linkov et al., 2013b; Collier et al., 2014). The existing compartmentalization might be a result of using analytic reduction for managing organizations, methods inherited from an era with limited connectivity and complexity. As mentioned in the introduction, IT has dramatically changed both connectivity and complexity of supply chains. Cyber-resilience has been described to be "*as much working with existing technology as it is about secure technology*" as "*cyber-resilience has less to do with information protection and more with operational control and trust in systems*" (Hult et al., 2014) thus involving human and technological development. Compartmentalization has been described as penetrating even the strategic levels of the company, as can be evidenced by the few IT experts ending up on company boards outside the technology sector (Herrington et al., 2013).

Another important evidence of compartmentalization is the different disciplines where the knowledge about cyber-resilience is being advanced, which includes environmental management, engineering infrastructure, and cybersecurity (Linkov et al., 2013). As a result, there is a perceived lack of integration for effective management of cyber-risks across disciplines and across departments, and as a result across decision domains, allowing for only incremental improvements in the management of these risks.

A *static approach* is one that does not consider time, particularly variation over time, as its main focus. The static characteristic of cyber-resilience frameworks is highlighted by authors through the problems this approach generates, resulting in that "*most companies do not know how to respond to cyber-risks in real time*" (Boyson, 2014), indicating that "*traditional static risk assessments are expected to become obsolete as new technology and methods become available"*, (Collier et al., 2014). More than 50% of the models found in the SLR did not make a reference to change in time as a relevant factor and thus are not able to consider real-time reaction. Other authors mention the need for situational awareness which is the "*perception of the elements in the environment in time and space, the comprehension of their meaning and the projection of their status in the near future*" (Abraham et al., 2015). This is required to counteract the "*velocity in cyber-attack spread*" (Tran et al., 2016). Velocity is a concept that is invisible to traditional static methods.

The *historical-dependence* of traditional cyber-risk assessment methods incorporate history in aspects such as probability calculations, and this was present in 66% of the quantitative methods for cyber-resilience proposed in literature as found through the SLR (McQueen et al., 2006; Fink et al., 2014) The problem with history-based methods is that "*cyber domain changes are so quick that there is no historical data for potential threats*" (Collier et al., 2014), as "*cyber threats cannot be clearly identified and quantified through historical measures due to the rapidly changing threat environment*" (DiMase et al., 2015). It is, therefore, is likely that "*companies will have to face unexpected risks for which no mitigation strategies had been planned in advance*" (Urcioli, 2015).

The *suitability of methods* refers to how these methods address the characteristics of cyber-risks to manage the response to disruptions from cyber-attacks. No discussion was found in the data in the synthesis sample about the suitability of the proposed methods because 1) no literature review was found that discussed cyber-resilience frameworks: Only Khan et al., (2015a) made reference to existing resilience frameworks in supply chains with limited references to their suitability for managing cyber-risk and resilience, 2) only 10% of the articles in the synthesis sample made a reference to resilience frameworks in other disciplines, and 3) no discussion was found to the particular characteristics of

cyber-risks, if any, to determine the suitability of the suggested methods.

2.9.3 Gap type 3: the people using the methods

With respect to the people using the methods for managing cyber-risk and resilience in supply chains, some authors mention the failure to develop IT security education at a sufficient scale, which now is affecting how cyber-resilience is understood among users, highlighting as an example the low level of literacy among UK civil servants about internet or cybersecurity (Herrington et al., 2013). This gap in the needs for cyber-literacy in an organization can render other cyber-resilience measures useless or inadvertently help propagate the effects of a cyber-attack (Chaves et al., 2017).

2.9.4 Further research questions

The gaps found in the SLR for answering the main research question give rise to new research sub-questions to guide the development of this thesis research. The questions derived from the gaps found in the analysis are shown in Table 14.

Table 14 Potential research questions from gaps in SLR

Concept	Gaps from SLR	Research sub-question
The cyber-risks being managed	Long reporting cycle of incidents	How can the available knowledge about cyber risks be quickly shared for better management?
	Unreliable reporting of incidents	How can the reporting reliability of cyber risks be improved?
	Underreporting of incidents	What incentives can be implemented for companies to report cyber-incidents?
	Mechanisms of action from cyber-attack to operational disruption	How do cyber risks cause operational disruption in supply chains?
The methods being used to manage cyber risks	Compartmentalization	What comprehensive methods can be used in supply chains for cyber risk and resilience assessment?
	Static frameworks	What dynamic methods can be used in supply chains for cyber risk and resilience assessment?
	Historical frameworks	What non-history dependent methods can be used in supply chains for cyber risk and resilience assessment?
	Suitability of methods	How suitable are cyber-resilience management methods to the characteristics of cyber risks
The people using the methods	Knowledge Gap	How can the cyber-literacy in supply chains be improved?

The main research question of this thesis points to the methods that can be used by organizations to manage security from and

response to cyber-risks, by deriving tools and techniques through which supply chains can prepare for, and react to disruptions to their physical operations from cyber-risks.

From the gaps that have been outlined in Table 14, the main research with respect to methodology corresponds to the suitability of the methods, compartmentalization of methods, static nature of methods and history-based characteristics of methods used for managing cyber-resilience.

The structuring of the research question(s) and sub-question(s) is essential for helping the stakeholders understand their problem better, and for keeping them interested and focused on a problem they care about (Booth et al., 1995), and, as in other business disciplines, scientific success in the research of SCM is to a great extent determined by the practical relevance of the results (Freimann, 1994).

Therefore, the answer to close the research sub-questions must be relevant to companies that are struggling to make sense of the apparent contradiction found in being exposed to an increasing cyber-threat landscape despite existing R&RM processes.

As a result, the research sub-questions that are pursued further in this research are broken down into two objectives. First, understanding the nature of cyber-risks and how these differ from other supply chain risks. To understand the particular

characteristics of cyber-risks to supply chains, a first research sub-question is proposed:

> *Research sub-question 3 (RSQ3): How do cyber-risks cause operational disruption in supply chains, and how does this differ from other supply chain risks?*

This composite question RSQ3 addresses the partly the SLR gap regarding the thing being managed, with respect to mechanisms of action, and the SLR gap regarding the methods being used, in respect to the suitability of methods (see Table 14).

Second, proposing tools from the systems thinking point of view, appropriate to the nature of cyber-risks that address some of the gaps found in current response management methods available to supply chains. The use of systems thinking as a framework for proposing the tools is explained in depth in the Methodology chapter of this work. Therefore the following research sub-question is proposed:

> *Research sub-question 4 (RSQ4): How can a systems approach be used to mitigate compartmentalization, static frameworks and historical-dependence for managing cyber-risks in the supply chain?*

As a result, the overall structure of enquiry for this thesis becomes the one represented in Figure 2, as shown in the Introduction of this thesis.

2.10 Thesis structure to answer the research questions

The chapters in this thesis cover the research questions as indicated in Figure 19. This figure also shows the relationship of each chapter to answering the research questions.

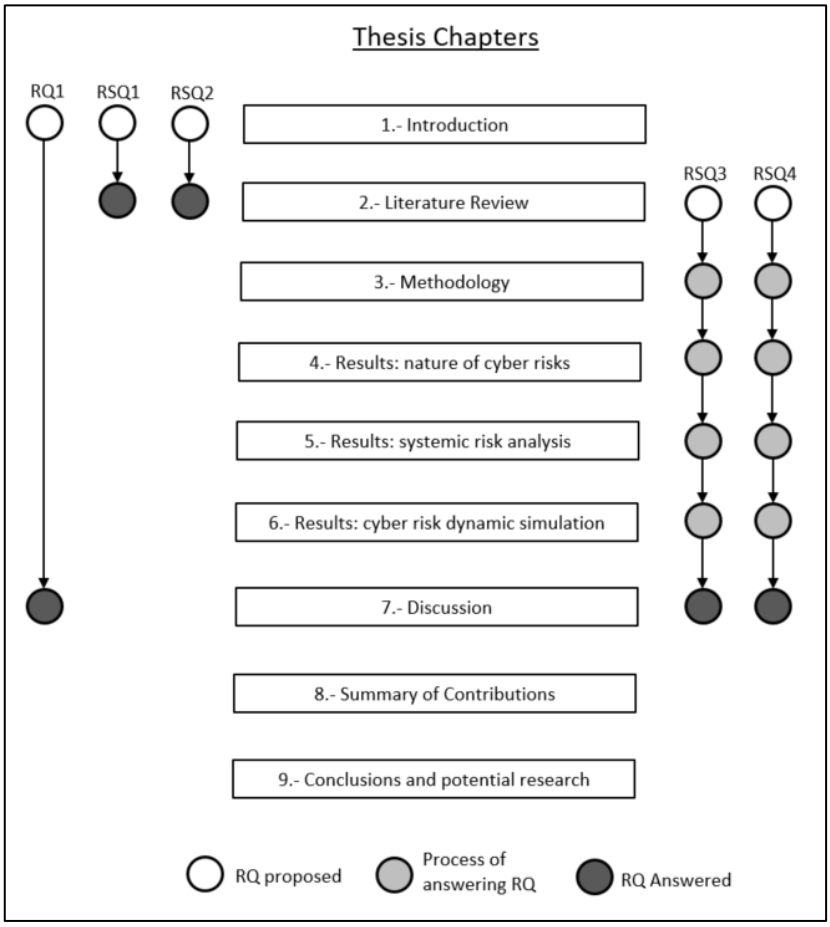

Figure 19 Structure of this thesis

2.11 Summary of the chapter

This chapter provided a background for the literature review process, described the suitability of carrying out an SLR, identified the biases present in the review process and outlined the choice of systems thinking as the framework through which the literature review is analysed thematically.

Furthermore, this chapter described in detail the systematic literature review method used, and presented the results, first in descriptive terms and then thematically.

Finally, the initial research sub-question are answered, relevant gaps found in the literature are outlined, and the remaining research questions and strategy of enquiry was completed which the rest of this thesis proceeds to answer.

The process of answering these research questions follows a process derived from a specific worldview or philosophical position. This position and the subsequent derivation of chosen processes for answering the research questions are described and explained next in the methodology chapter.

3 Methodology

This chapter describes the need for a clear methodology as an essential part of sound scientific contributions, and gives a detailed account of the methodologies followed in this thesis work.

The chapter starts by discussing the strategic aspects: the philosophical position taken throughout this study followed by the explanation of the approach to theory development chosen for this work, also known as the “logic” of the research. Thereafter the design aspects are discussed: the methods used for the research are explained and arguments for their choice are given. The chapter continues with an explanation of the strategies considered in the research, to then finalize by explaining the tactic aspects of this research, namely the data collection and data analysis methods for each of the research questions, and the considerations for the quality of the research are laid out.

3.1 Relevance of the methodology

In order to answer the research questions, specific processes are followed, based on assumptions concerning the nature of the problem and the proposed ways/methods in which these gaps can be closed and how a theoretical contribution is made from this process. This chapter deals with the methods used in this thesis, the philosophical foundation upon which these methods were

chosen, as well as a critical analysis of their advantages and limitations.

Having a clear, explicit and consistent framework for analysing the methodology followed in this work, is a fundamental starting point from where knowledge can be built in a coherent way. Boer has proposed that, due to the need of embracing the epistemological diversity present in the operations management research community, a meaningful contribution proposal does not necessarily rely on following a strict set of criteria, but rather through consistency (Boer et al., 2015). As Jonathan Grix put it, "*research should be judged on how its constituent parts logically link together, and not by which methods are used*" (Grix, 2002).

The framework used in this thesis for structuring the methodology proposal and thus ensuring consistency is based on the "research onion" as proposed by Saunders et al., (2016). This approach for framing the research project framework is based on a layered understanding of the conditions and assumptions that lead to the specific chosen research configuration. The choice in each layer serves both as input and border conditions of the available choices for the subsequent layers in the configuration. The layers considered through this research structuring approach are 1) the research philosophy, 2) the approach to theory development, 3) the methodological choice, 4) the strategies and the time horizon and finally, 5) the techniques and procedures that

are followed. A graphical representation of the onion can be seen in Figure 20.

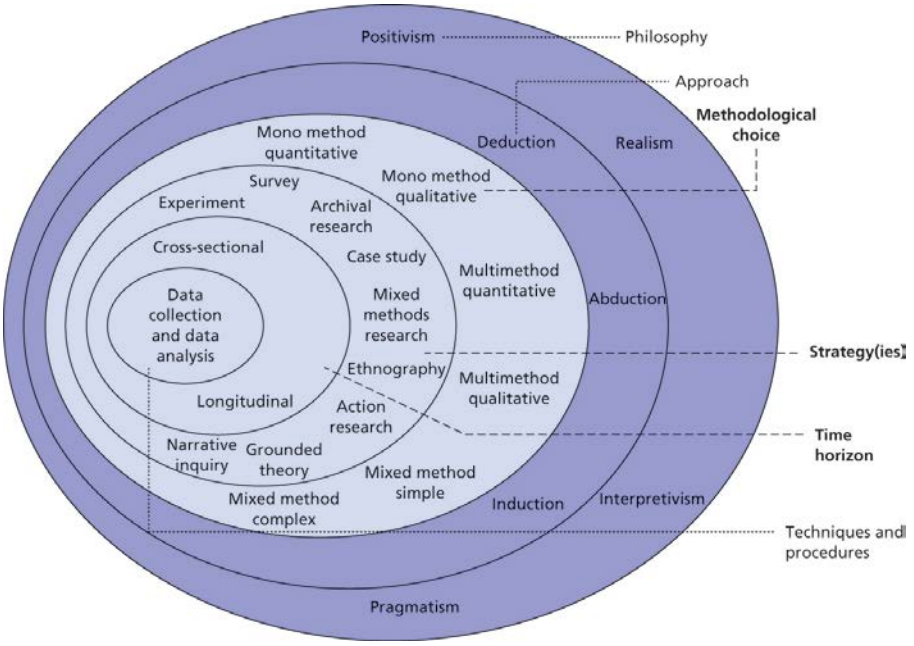

Figure 20 The research "onion" (Saunders et al., 2016)

Therefore, in following the "research onion" approach to understanding research, the methodology chapter starts with a detailed overview for each of these methodological "layers.

Based on the description of the complexity that characterizes the topic of cyber-risk and security in the global supply chain, the approach followed in this thesis work is that of systems thinking. It was already introduced briefly in the literature review chapter when detailing the analysis framework, but its choice is justified in detail in this chapter. Furthermore, the methodological implications of choosing systems thinking for this work are

described, from the philosophical position down to the data gathering procedures.

3.2 Systems thinking theory

This section explains in a concise manner the foundations and philosophical implications of systems thinking and of the methodology of System Dynamics (SD). Considering that SD has been explored by an active community for many decades having implementations in different areas of human activity and influence, only the essential aspects of the systems thinking and SD are reviewed in this section of the thesis, as these are needed to understand the assessment tools being used to advance theory and answer the research questions later in this work. Therefore this exposition represents a limited view of what SD has to offer.

Readers interested in deepening their knowledge beyond what is presented in this thesis are encouraged to refer to the works by Forrester (1961), Randers (1981), Richardson (1991), Bossel (1994), Sterman (2000) and Meadows (2008), and to reach out to the System Dynamics Society[2] and the Creative Learning Exchange[3].

[2] http://www.systemdynamics.org

[3] http://www.clexchange.org

3.2.1 Background

Systems theory is an approach that started in the late 1930's by the combination of emergent ideas from different fields into a general theory of systems, combination advanced by from Norbert Wiener (1948) from the control and communications engineering knowledge domain, and later by Ludwig von Bertalanffy (1968) from the biology knowledge domain, the latter being recognized as the founder of this movement (Leveson, 1995). Von Bertalanffy argued that the classical conceptualization of a closed system according to thermodynamics was not applicable to large classes of phenomena. Systems theory was born therefore as a response to certain limitations of traditional science at the time for coping with complexity.

Traditional science is based on the precepts of repeatability and refutation, both of these based on the principle of analytic reduction, also called "*reductionism*". Analytic reduction, credited to Rene Descartes (1596-1650), postulates that problems can be divided into identifiable parts, and then each part can be examined separately, making in the process three important assumptions (Checkland, 1981):

- Dividing the problem into components does not distort the phenomenon being studied,
- Every component is the same when examined on its own as when it is part of the whole, and

- The principles governing the interaction of the components is straightforward.

These assumptions are reasonable for a big group of systems with physical regularities, and which has been described as having "*organized simplicity*" (Weinberg, 1975). For these systems, the interactions between components are known, and the interactions can be examined in pairs, limiting the number of possible interactions. This allows the system to be separated into subsystems without affecting the resulting behaviour of the system. Structural mechanics in physics has been highly successful in applying this model to systems in theory development.

The second type of system is those said to have "*unorganized complexity*" (Weinberg, 1975), which do not have a clear underlying structure for the application of reductionism. These systems are then treated as aggregates, considering them complex but regular, and an understanding is gained by treating them as exchangeable units and calculating some mathematical moment, such as averages or standard deviations for some behaviour of interest. The basis for this approach is the "*law of large numbers*" whereby the larger population being studied, the more likely that the observed values are close to the predicted average values. For example, statistical mechanics is an example of the application of this approach.

However, there is a third type of system which exhibits what has been called "*organized complexity*" (Weinberg, 1975), which have been identified as those systems that are too complex for a complete analysis, but too organized for statistics. Systems exhibiting organized complexity describe many of the engineering systems that have been created post World War II, as well as biological systems and social system, and all these are the subject of systems thinking theory (Leveson, 1995).

Moreover, the combinatorial complexity that has been described above, also known as detail complexity (Sterman, 2000, p.21), i.e., the complexity derived from the number of system components and relationships, is not the only complexity possible. Dynamic complexity arises from the interactions among the system components over time. Therefore dynamic complexity can arise even in systems with low combinatorial complexity. This dynamic complexity arises because (Sterman, 2000, p.22):

- Systems are *dynamic*, i.e., their structure changes over time,
- Systems are *tightly coupled*, i.e., the components of the system interact constantly
- Systems are *governed by feedback*, as the actions of a system modify the state of the system and its environment, which in turn condition future decisions. Dynamics are the result of these feedbacks (Richardson, 1991),

- Systems are *nonlinear*, as the effect on the behaviour is rarely proportional to the cause,
- Systems have *delays*, as the effects are not necessarily expressed right after the cause,
- Systems are *history-dependent*, where future decision options are conditioned by the decisions taken before, and some of those decisions are irreversible, i.e., those decisions cannot be undone,
- Systems are *self-organizing*, inasmuch as their dynamics are borne from its internal structure,
- Systems are *adaptive*, as they react and change decision rules of the constituent agents over time.
- Systems are *counterintuitive*, partly due to cause and effect being distant in space and/or time, partly because attention is drawn rather to symptoms than to underlying causes,
- Systems are policy resistant, derived from the complexity of the systems in which human activity is embedded, overwhelming the intuitive ability to understand them; as a result, apparently obvious solutions result in a deteriorating situation,
- Systems are characterized by trade-offs, as the delays present result in a behaviour in the long run that is different from the short-term results. Worse-before-better behaviour is a result of this when immediate yet transitory

> performance deterioration gives way to performance improvements in the long run, or vice versa, known as "better-before-worse behaviour" (Sterman, 2000), when immediate yet transitory improvements are followed by long-run system performance deterioration.

Systems thinking has a focus on understanding systems as a whole rather than about their parts separately, and it considers that there are system properties that can only be understood correctly taking into account social and technical aspects (Ramo, 1998; Sterman, 2000). These system properties are generated by the relationships of the parts that constitute the system, such as their fit and interaction. Therefore a systems approach focuses on the analysis and design of the whole instead of the components or the parts.

Systems theory is based on two pairs of ideas: emergence and hierarchy, and communication and control (Checkland, 1981, Leveson, 1995).

A system can be organized in increasing levels of complexity, where a higher level is said to have a higher level of complexity as well, and encompassing greater aggregation. This approach allows for the identification of *levels of hierarchy*, where each level is characterized by *emergent properties*, i.e., those properties that would be meaningless in a lower level, but which can be used to describe a higher level of the hierarchy. For example, the shape

of an apple is an emergent property which would not be understood when analysing the apple at a molecular level, as it is the result of a complex network of interactions at the molecular level, and which can only be observed when understanding the system from a higher level of the hierarchy. In the same way, supply chain cyber-resilience can be considered an emergent property that cannot be understood from the individual transactions between the components of the supply chain, but is the result of a complex network of interactions at the individual transaction level, and which can only be understood from the supply chain level of hierarchy.

The constraints imposed on a specific hierarchical level from a hierarchical level above it, which define the ways in which that lower level can behave, are the "*control actions*" effected between hierarchical levels. As such, the application in man-made systems of the control mechanisms seen in natural systems has been studied by a branch of systems theory known as "*cybernetics*". Therefore the description of control processes "*necessarily required taking into account at least two levels of hierarchy*", and as such, "*the upper level is a source of an alternative and simpler description of the lower level in terms of specific functions that are emergent as a result of the imposition of constraints*" (Checkland, 1981).

The phenomenon of control in open systems (i.e., those that have inputs and outputs from the environment) introduces the need for *communication* of information for regulation and control: the information is obtained from the controlled process through some form of sensor, and the process is influenced by communicating information through some type of actuator, as it can be seen in Figure 18. In that figure, communication takes place in the cyber-physical as well as the socio-technical level, and the algorithms and set points provided by the human controller to the SCADA system (see section 2.7.6), correspond to the control actions effected by the socio-technical hierarchy on the cyber-physical hierarchy.

If this reasoning progresses from the system controlling some physical process to higher levels of hierarchy, these higher levels would sequentially consider operations management as a higher hierarchy to the process control, as it looks at different controlled processes; company management as a higher hierarchy than operations management as it considers different parts of the company; governmental regulatory authorities as a higher hierarchy than company management as they consider different companies in their geographical influence, and so on.

Leveson (2011) developed a generalized representation of this generalized hierarchical control system, represented in Figure 21. Every hierarchy determines operational boundaries for the lower

levels and receives information from the lower levels as well. Therefore, the level of aggregation, i.e., the hierarchy level that is chosen to model a system is conditioned by the questions that are to be answered.

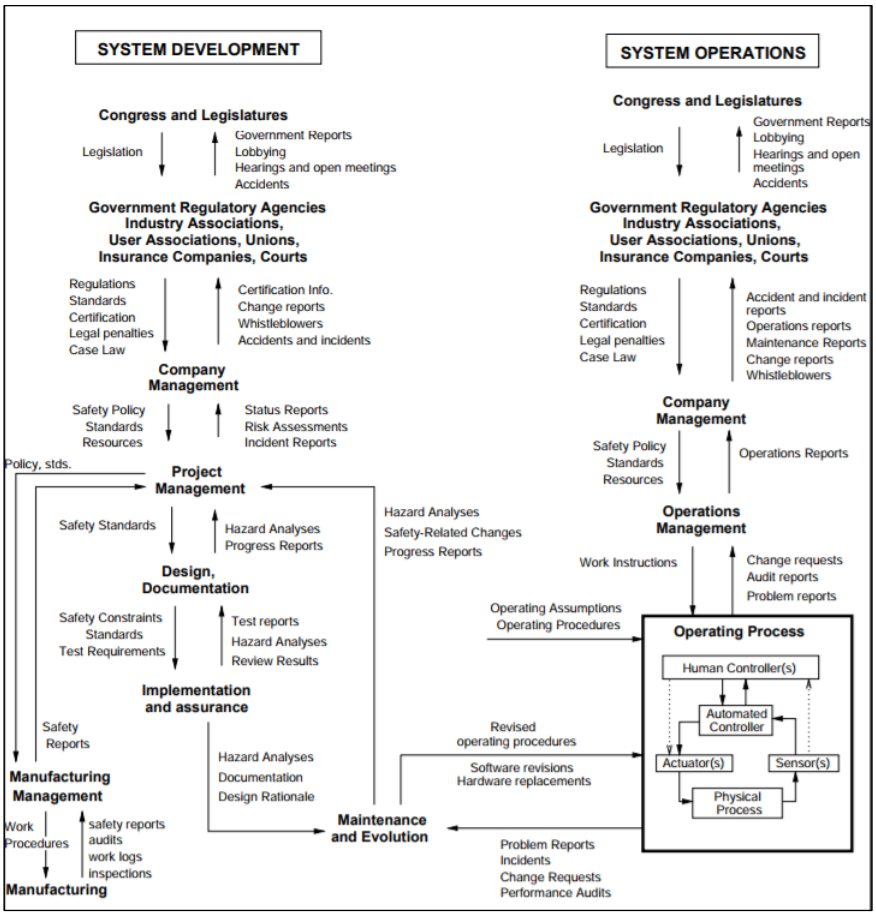

Figure 21 Hierarchy of a sociotechnical system (Leveson, 2011)

3.2.2 Basic definitions

In order to build the foundation of systems thinking as applicable to this thesis, some definitions are necessary (Forrester, 1961; Bossel, 1994; Sterman, 2000).

- The *system* has been defined as "*a set of components that act together as a whole to achieve some common goal, objective or end*" (Leveson, 1995). The assumptions required for this definition include that the goal of the system can actually be defined and that the structure of the system can be identified as a series of components with relationships between them (Mihramber, 1972). Moreover, Bossel (1994) argues the system's purpose has to be recognizable by an observer, thus making the *analyst* also an explicit part of the systems thinking conceptualization. This can be said to be the basis of the *idealist / presentationalist* philosophy (Olaya, 2009) underlying systems thinking.
- The *state* of a system is given by a set of relevant quantities that completely describe the system at that specific time. These states are independent of each other, and the number of state variables that are needed to make an essential description of the system at a specific point of time is said to be the *dimension* of the system.

- The *environment* for a system is the set of components that despite not being part of the system are able to affect its state. The system is separated from its environment by a boundary.
- The *structure* of a system is the set of essential components and relationships that form the system. These relationships and components are said to be essential since any division of the system (i.e., loss of any of these essential components or relationships) would not allow the system to fulfil its goal.
- *Inputs* and *outputs* from the system are anything that crosses the boundary between the system and its environment

A system is "*an abstraction conceived by an analyst*" (Leveson, 1995), who defines the system boundary, the components of the system and their structure, and the inputs and outputs of the system, additional to the goals of the system as mentioned earlier. These concepts are represented in Figure 22.

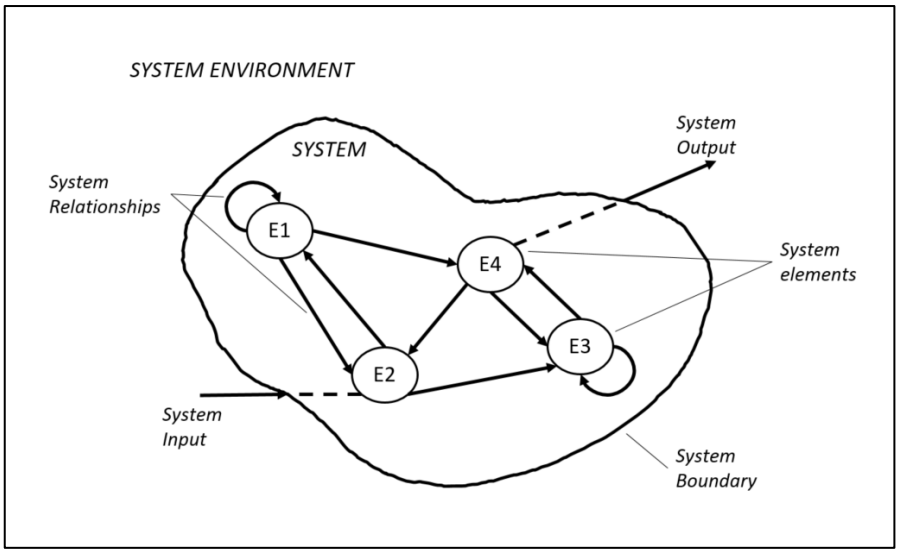

Figure 22 System concepts (based on Bossel, 1994)

Now, given the definition of a system to be observable to the analyst, a relevant question is "when is a system observable? Bossel (1994) argues that this only happens when a system acts on the surrounding environment by some behaviour or output variable, and that if this output variable does not correspond directly to changes in the environment, then these output variables must have been caused by something within the system itself, i.e., changes in the state of the system, described by the state variables.

As a consequence, a system according to the systems thinking theory differs from a system in the thermodynamic sense as the latter considers a system materially closed and causally open, the systems thinking approach seeks to understand systems as materially open and causally closed (Sterman, 2000).

As a way of understanding the world through systems, it is not only relevant to understand how these are built, but also how they react over time, i.e., their dynamics. The next section presents how this variation over time can be represented and analysed, by using a method known as system dynamics.

3.2.3 System Dynamics basics

All systems upon closer inspection, are dynamic, i.e., their states experience change over time, albeit some of them slowly. The change in the state of a system over time is known as its behaviour. However, "*frequently, knowledge about past system behaviour is not sufficient for obtaining reliable statements about future system behaviour*" (Bossel, 1994), a particularly relevant insight for cyber-risks in the global supply chain.

Forrester (1961) started what can be called the "*MIT School*" of thought in SD modelling. He brought together three fields which at that time were relatively new: Control Engineering through concepts such as feedback and self-regulating systems, Cybernetics through concepts such as the nature of information and the role it has in controlled systems, and Organizational Theory by considering the structures present in human work groups and the nature of decision-making.

SD is a framework and methodology for the representation of systems that change over time by using networks of variables in

relationships of circular causality. These networks are composed of fundamentally two types of variables: stocks (accumulations) and flows either flowing into or out of these accumulations. By virtue of different timescales or the specific problem under question, it is sometimes convenient to represent some of these stocks or flows either as constants, i.e., not changing within the constraints and timeframe of the problem being analysed, or as auxiliary variables, i.e., changing instantaneously.

The visible "*state*" for such a system is therefore completely represented by the values of the stocks in the system and all changes in these stocks are what can be understood as the system's "*behaviour*". These conditions have two consequences: 1) by virtue of this networked representation, all the behaviours of the system are the direct result of its own structure, in what is termed the "*endogenous*" view of behaviour in SD, and 2) any system that changes over time in an interesting way, has at least one feedback loop, i.e., the basic circular causality unit, in its structure (Forrester, 1961). SD is thus said to represent systems that are "*materially open*" and "*causally closed*" (Sterman, 2000).

The relationships between variables in a system dynamics model can have any functional form, and be linear or non-linear. In the case of supply chains, non-linearity arises from the interaction between the physical and the institutional structure of

that system with the decision making processes of the agents acting within it.

As an example consider the process of keeping stock of "*widgets*" in a supply chain. The supply chain would have a certain amount of stock that increases with the production of this stock (manufacturing or purchase) and the amount of stock would decrease through the use or shipment of this stock. This would be represented as a stock and flow diagram composed of one stock or level, "*Inventory*", one flow going into this stock, "*Production*", and one flow going out of this stock "*Shipment*", as shown in the next figure.

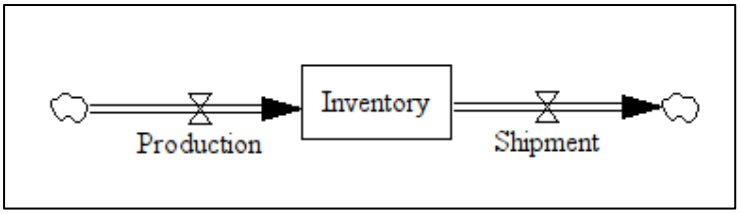

Figure 23 Stock and flow diagram

The "*clouds*" at the extreme of each of the flows represent the limits of the system as it is currently considered. These limits are determined by the group that is developing the model, and it is a representation of the mental model this team has on the boundaries of the problem, and are a representation of the "*materially open*" nature of system dynamics models. Given that a system dynamics model is causally closed, all relevant events in the system have to be explained with what has been considered within the clouds.

Otherwise, the limits of the system have to be revised and modified, in a process denominated in the SD community as "*challenging the clouds*" (Sterman, 2000), approach applicable to a broader spectrum of life, as the philosophical position of constantly challenging self-imposed limits.

The Inventory stock is the result of the inflows through Production and the outflows through Shipment. This means that the mathematical representation of these elements and their relationship can be either through a differential or an integral equation. The integral equation accounts for the value of the stock "*Inventory*" as the accumulation over time of the inflows minus the outflows.

Equation 1

$$Inventory(t) = Inventory(t_0) + \int_{t_0}^{t} (Production(s) - Shipment(s))ds \quad [Widgets]$$

On the other hand, the differential equation focuses on the rate of variation of the stock, as resulting from a net change of the inflow minus the outflow.

Equation 2

$$\frac{dInventory}{dt} = Net\ change\ of\ Inventory = Inflow(t) - Outflow(t) \quad [Widgets/week]$$

The use of stocks is extremely relevant as Nathan Mass (1980) through his study of the dynamics of stock and flow variables applied to the problem of supply and demand. He identified stocks are critical in creating changes over time (dynamics) in systems as:

- Stocks provide a *characterization of the state* of the system that is modelled, thus providing a base for decision-making. The state of a supply chain may be reflected by the level of inventory held at each step of the chain. Changes in these levels, when compared with desired levels, lead to specific actions in the case of a low Inventory level, a possible decision is to increase production, thus increasing the inflow to this stock.
- Stocks *provide inertia* to the system, and constitute the system "*memory*". Since the stocks accumulate past events (as represented by the net flows) if the activity is suspended and later restarted, the stock continues to represent the latest condition that was reached by the system, and from which the activity can proceed. The quantity of defective inventory, for example, remains the same until the time when either this stock is decreased by the elimination of defective inventory through actions such as sales or rework, or this defective inventory stock is further increased by defective production processes.

- Stocks *result in delays*, understood as the process where an output has some lag to the corresponding input. For example, in the case of a supply chain with a stock of inventory, there is some average lag between the time when an item enters the stock (i.e., it is produced) and the time when this item is shipped from the inventory. This average time is zero only in the case where no stock is kept, being this the case of pipeline flow, just in time, or make-to-order manufacture.
- Stocks *decouple the inflow and outflow* rates allowing dynamic disequilibrium to arise, this being the fundamental source of dynamics in a system. Stocks accumulate the difference between the inflows and outflows and thus a stock allows these two processes to differ. If the Inflow is greater than the outflow, the stock increases and if the outflow is greater than the inflow, the stock decreases. If the outflow and inflow are equal, then there is no change in the stock level (the same amount is entering the stock as it is leaving it). This unchanging stock level even though there are flows, is called a "*dynamic equilibrium*". This differs from the "*static equilibrium*" which is the case when there is no flow, and thus no activity in the system. For example, take the case of the Department of Management Engineering at DTU. If there are the same number of students graduating from DTU Management Engineering as

there are entering a study line in the same department, then the number of students remains the same, and this system is said to be in dynamic equilibrium. Since these two activities are controlled by different decision-makers in the organization, a buffer such as a "*stock*" of available studying facilities, needs to exist to allow these two decision processes (admissions and graduation) to differ.

Furthermore, in the case of this example, the production level is not independent of the level of inventory but rather seeks to comply with the desired inventory level. This is represented by the following figure.

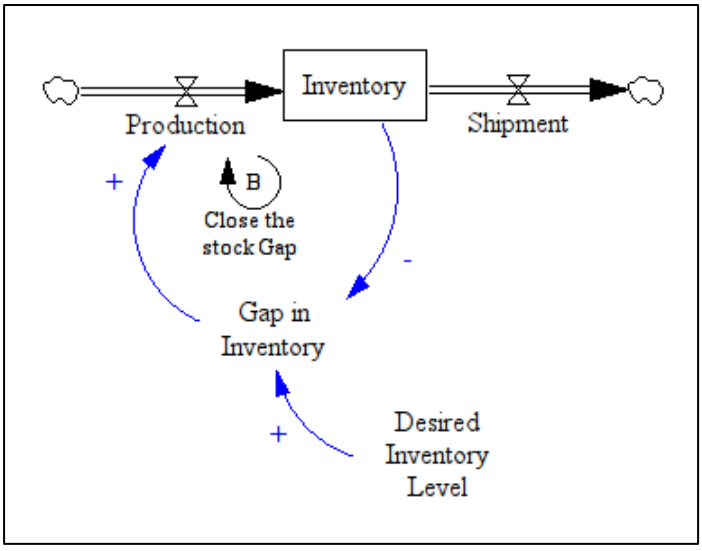

Figure 24 Feedback Loop example

In this case, two additional variables are included in the model. The first one is the "*Gap in Inventory*" variable, which reflects the difference between the desired and the actual inventory levels.

The second is the Desired Inventory Level, which as a first approximation it can be considered as a constant.

Equation 3

$$Gap\ in\ Inventory = Desired\ Inventory\ Level - Inventory$$
[Widgets]

Equation 4

$$Desired\ Inventory = constant$$
[Widgets]

The following structural features of the representation in Figure 24 have to be noted:

- There are *causal relationships* that have been added, represented by arrows with either a positive or a negative sign. These are called the "*polarities*" for these causal relationships. A positive polarity indicates that the two variables behave in the same way, i.e., if one increases, the other one increases as well. In the same way, if one variable decreases, then the other variable also decreases. For example, if the Gap in Inventory increases, then the Production also increases, but additionally, if the Gap in Inventory decreases, Production would also decrease. A negative polarity reflects cases where two variables behave in opposite ways. For example, if the Inventory level increases, then the Gap in Inventory decreases, all else

equal. In the same way, if the Inventory level decreases, then the Gap in Inventory increases, all else equal.

- There is a *circular causality structure* that was added to the model, namely the one considering the loop formed by Production – Inventory – Gap in Inventory. This is a Feedback loop which connects these three variables in a sequence of mutual influence. The nature of this Feedback loop is determined by the polarities between the variables that are part of this feedback loop. In this case, it is a Balancing feedback loop, also known as a negative feedback loop, as the net effect of the circular causality is to counteract variations in any of its constituent variables. For example a decrease in the inventory level would lead to an increase in the Gap in Inventory level (mediated by the negative polarity between these variables). Then an increase in the Gap in Inventory would lead to an increase in Production (mediated by the positive polarity between these two variables). Finally, an increase in Production would result in an increase in the Inventory (there would be greater inflow into the Inventory stock, all else equal). The resulting effect of this balancing loop when faced with a decrease in Inventory, is actually to increase Inventory levels. This increase continues until the gap is zero, i.e., until the Inventory level has reached the desired inventory level, which is the goal of this balancing feedback loop. The

other possible circular causality structure (not present in this simple model) is a reinforcing feedback loop, also known as a positive feedback loop, as the effect it has is to compound and amplify variations in its constituent variables.

- The representation has an indication of the *loop type as well as a distinctive name*. This is not merely aesthetic, but relevant for at least two reasons. First, the labelling of the loops in the diagram can help locate the loops involved in the behaviour as extracted by the analyst. This can be advantageous when the models grow to have a greater number of loops. Additionally, the names that are assigned to the loops help greatly in communicating the storyline behind the behaviour as identified by the analyst.
- *Exogenous* and *endogenous variables* can clearly be identified from the diagram. Those that have an arrow, be it a causal arrow or a flow, are said to be "endogenous" to the model, as their value is defined by some other variable in the model. On the other hand, those variables that have only an arrow going away from them, are "*exogenous*" to the model, as these have to be determined externally. These two categories are relevant at the time of experimenting with the model and defining intervention policies, as it is exogenous variables that can be changed to see different model behaviours. The only way of changing endogenous

variables would be through structural changes, i.e., by changing the causal relationships between existing variables or by introducing some new exogenous variable that would modify the endogenous variable.

- The analysis that is carried out for this model as is the case of any other SD model, is only looking at one causal relationship at a time, holding all else constant, i.e., the ceteris paribus condition of analysis for SD models.

The general representation of an SD model and summary of what was explained from a practical model is shown in Figure 25. The state of the model, as represented by the levels or stocks in the system, is the information that feeds into the flows, or decision points, and which are a result of the policies chosen by the organization. These policies are influenced by a goal (that need not be a constant, but in itself be influenced by other policies), and this decision making, in the form of an action, creates a change in the level, where this process is repeated continuously.

Information in the system does not deplete its source, however, rates/flows do. Information flows are not conserved quantities. For example, the information about levels of inventory can be used to determine how much new inventory to buy and at the same time used to determine the required warehousing space. On the other hand, the network of connected States/Levels and Rates/Flows are conserved: an outgoing flow from a stock,

decreases this stock, and an incoming flow into a stock increases this stock. For example, the selling and shipment of existing inventory decrease the available inventory, and the purchasing of inventory increases the inventory stock.

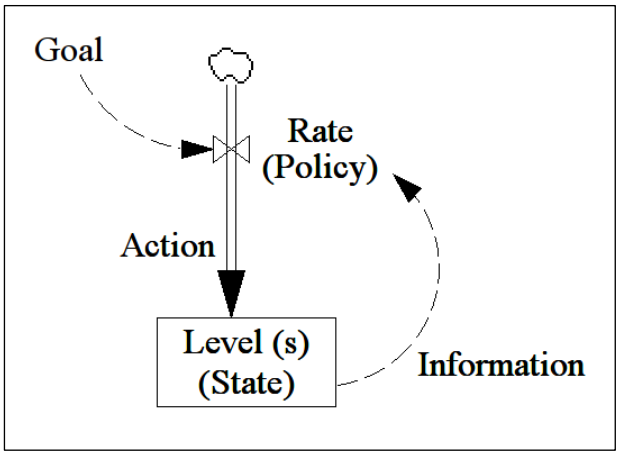

Figure 25 SD general model

Forrester proposed outlined a modelling process in his seminal work “Industrial dynamics” (Forrester, 1961). Additional to this original modelling process, other generic SD model development processes have later been proposed by Randers (1980, p.119), Richardson and Pugh (1981, p.16), and Sterman (2000, p.86). These show differences in the emphasis assigned to specific stages, but all agree in describing the process as an iterative, constructivist approach. Martinez-Moyano (2013) explored these differences to subsequently propose an overarching development framework, which includes novel aspects, such as including both

the strategies and infrastructure required for learning, an aspect not previously considered as an explicit part of the methodology.

Bossel (1994, p.12), from what can be called the "German school" of thought in system dynamics modelling, puts forward a process for model development, simulation and behavioural analysis during system design, directed towards systems in general, including social systems, where he included the mathematical analysis as an explicit step in the process. This is not explicit in the MIT School of thought, and connects Bossel's approach much more to its engineering background, in contrast to the engineering management background that influenced the MIT Sloan School, where Forrester developed his industrial dynamics approach. Bossel's approach lays a special emphasis on finding state equations, equilibrium points, attractors, stability and behaviour at equilibrium points, for example (Bossel, 1994, p.20).

Bossel has worked extensively in the wider application of system dynamics beyond sociotechnical organizations to domains such as predator-prey interaction, classic control problems in mechanics and hydraulics, hydro-thermodynamic equations such as the Lorenz system, and mathematical applications such as chaotic attractors.

The SD development strategy that is used in this work follows Sterman (2000) and is an iterative process according to the generic steps of problem articulation and boundary selection, dynamic

hypothesis formulation, model formulation, testing, and policy formulation and evaluation.

During problem articulation, the main aspect to be resolved is determined, and an assessment is made about the real underlying problem, beyond merely its symptoms. A model purpose is identified and the system boundaries are chosen. Additionally, an initial characterization of the problem is made, through tools such as time horizon and reference mode identification. The reference modes represent the problem dynamically i.e., through patterns of change for relevant variables over time as represented by graphs and other descriptive data. The iterative model development process goes back to these reference modes to confirm an alignment between the model development and the model objective is maintained. On the other hand, the time horizon for the problem is constituted by all the time required to describe how the problem emerged and to describe its symptoms, extending sufficiently far into the future to include delayed effects, even if these are indirect. The choice of an adequate time horizon is not trivial, as one of the deficiencies in the mental models of the world is the tendency to consider cause and effect as local and immediate, while these may, in fact, be located far away from each other physically and happen with some delay from one another. Additionally, the choice of the time horizon for the problem can also have a relevant effect on the perception of the problem.

The dynamic hypothesis is developed after the problem has been defined over an appropriate time horizon, and it is a theory that explains the troublesome behaviour in the reference modes. The dynamic hypothesis accounts for changes over time in the system referring to its structure is provisional, this is subject to revision throughout the iterative modelling process, and it aids and concentrates modelling efforts on certain parts of the model structure. The remainder of the modelling process is aimed at testing this dynamic hypothesis through experiments with the model and real-world data collection.

The dynamic hypothesis extracts the mental models existing in the organization related to the origins of the problem, and normally mediation and facilitation are crucial, as different members in the system have a different theory on how the problem came to be (Vennix, 1996; Andersen et al., 1997). A major characteristic of the dynamic hypothesis is that it needs to derive its explanation from the variables and interactions of variables present in the model, in what is known as the “endogenous” source of the behaviour, “endogenous” coming from the Greek that means “coming from within”. Through such an explanation, the system structure can be altered to reveal changes in the behaviour. The opposite of this would be an “exogenous” explanation of behaviour, by using external variables o explain behaviour. This is self-defeating as an explanation since the logical follow-up question would be then what made this exogenous variable

change. By seeking to explain this, the model is expanded and thus an originally exogenous variable would become endogenous.

The model formulation process relies on tools such as boundary diagrams, subsystem diagrams, causal loop diagrams (influence diagrams), and stock-and-flow maps. These diagrams serve as "*an intermediate transition between a verbal description and a set of equation*" (Forrester, 1961), and to be a tool for conceptualization, these have to efficiently organize the descriptive data held in the mental models, portrayed as the real decision-making processes (Morecroft, 1982). Table 15 summarizes the different available tools and some of their advantages and disadvantages.

Table 15 Main conceptualization tools used in System Dynamics

	Model Boundary Chart	Subsystem Diagram	Causal loop diagram	Stock and flow maps	Policy structure diagrams
Description	A summary of the boundary of the model by listing key variables, indicating those that are endogenous, those that are exogenous, and those that have not been considered in the model	A summary of the overall architecture of the model, representing subsystems and their connections.	A map describing the causal links between variables in the system, trough the use of arrows from a cause to an effect, polarities and feedback loops.	A map representing the physical flows of the system and the feedback structures present	Representation of the internal structure of a subsystem.
Advantages	By stating what has been left out, the boundaries of the model and its applicability are made explicit. It is the immediate result from an initial team brainstorming about the problem, can serve as a consensus tool.	States explicitly the subsystems, defining the level of aggregation of the model. It represents the coupling of the subsystems explicitly. Identifies exogenous from exogenous variables.	Useful in capturing hypothesis for the causes of dynamics, the mental models in the organization, and representing feedbacks. Differentiates between endogenous and exogenous variables. Integrates delays qualitatively. Widely used in scientific research.	Can be simulated computationally. Can represent subsystems and the level of aggregation of the model. Differentiates between exogenous and endogenous variables. Integrates aspects such as inertia and delays explicitely.	Represents explicitly stock, flow and information variables. Represents decisions explicitly.
Disadvantages	It shows no relationships between variables, does not identify stocks, flow and information variables or any feedback processes. Does not identify exogenous from endogenous variables.	Does not differentiate between stocks, flows or information variables. Does not indicate polarities and it does not indicate any feedback process. No explicit representation of what has been left out of the model.	These do not differentiate between stock, flow and information variables, and thus lead to polarity ambiguity. Little correspondence between mental model and loop structure. Seems like a conceoptualization tool, but is better suited as a summary tool of insights. No explicit representation of what has been left out of the model.	Very difficult to achieve, even for systems of medium complexity.	Has to be used in connection to Subsystem Diagram.

3.2.4 System Dynamics to Sociotechnical problems

Forrester´s approach in 1958 to understanding socio-technical systems considered aspects of the operations which had not been part of the models until then, "*the limited information flow across organizations and functions within organizations, delays in gathering information, making decisions as well as the implementation and impact of those decisions, and the behavioural, sometimes suboptimal decision rules managers used to make inventory and production decisions at each level of the supply chain*" (Sterman et al, 2015).

System Dynamics has been used to explore cyber-risks, though not with a focus on supply chains.

Radianti et al., (2007) explored possible structures and incentives present in a black market for vulnerabilities in digital communication systems. Their approach was exploratory and modelled aspects such as information asymmetry, stakeholder interaction and reward structures in the market. A more recent approach has been proposed by researchers at Harvard and MIT, with respect to zero-day vulnerabilities[4] (Siegel et al., 2015). Siegel does not explore the operations that lead to the availability

[4] See the glossary

of zero-day vulnerabilities and rather concentrates on the flow of decisions that lead to the accumulation and use of the available zero-day vulnerabilities. This is consistent with the most powerful focus of the SD methodology, which is *"… not on individual decisions, but on the policy framework producing continuous flows of decisions…"* (Richardson, 1991, p.158)

Gonzalez et al., (2017) have proposed ways of using System Dynamics for understanding the incentives that are present in IT Security Management, and their effect on system performance. By using system archetypes (Wolstenholme, 2003) and concept simulation models, and for electronic systems in the banking industry, they compare the effects of system performance when the end user has the burden of proof for an alleged cyber-attack, such as European banks, with respect to the North American model, where burden of proof corresponds to the bank. Their model concludes that an improved learning process is achieved in the latter.

3.2.5 Suitability of the System Dynamics method

SD is a framework offers advantages to understanding problems like the cyber-risks as these are being experienced by supply chains. These advantages can be catalogued as coming mainly from epistemological, technical, and flexibility dimensions.

Epistemologically, system dynamics is a representation which can be applied at different levels of aggregation and/or abstraction, being particularly well suited to problems of policy analysis. A distinguishing feature of the system dynamics method is the endogenous explanation principle, where the behaviour of the systems is a result of its structure:

"*System Dynamics […] regards external forces as there, but beyond control and hence not worthy of primary attention […] Instead, the focus is upon examining the organization's internal structure; the intent being to arrive at an understanding of how this structure […] can be made more resilient to environmental perturbation. In adopting this approach, system dynamics is embracing the wisdom of the human body. The body, rather than forecasting – and then marshalling its forces in anticipation of – the arrival of each kind of solid and liquid input, remains continually poised in a state of general readiness for whatever may befall it*" (Richmond, 1967).

Computer models are a powerful source of information if properly constructed, presenting several advantages with respect to mental models:

- Computer models are explicit representations with documented assumptions
- Computer models calculate the consequences of the assumptions without error or bias

- Computer models are more comprehensive than mental models, as these can interrelate many more factors than the human mind can

Computer models have also several shortcomings, as they are unable to deal with relationships between factors that are difficult to quantify, or that are difficult to replicate due to a lack of historical experience.

3.3 Research philosophy

Research philosophy refers to the way in which the knowledge is developed (Saunders et al., 2016). It incorporates beliefs and assumptions into the ways this research development happens and constitutes the cornerstone for the definition of a research process Beliefs and assumptions are at the same time ontological, epistemological, as well as axiological, and each of these is explained and defined for this research in the next section. In this way, the philosophical position that is considered in the research are made explicit, and its coherence is explained in this chapter. The choice of a research philosophy is not trivial since as it was shown through the research onion strategy, the philosophy influences the subsequent choice of methodology, research strategy, data collection techniques, and analysis procedures.

3.3.1 Ontological assumptions

The “ontological position” of a research is a concept that describes the assumptions present in the research about the nature of reality and its definition, by answering questions such as what this nature is, and what the world is like. An ontological position is defined in terms of how much of that nature is real and objective or nominal and decided by convention, how much of this reality is external to the researchers or socially constructed, how much of this reality is based on the existence of one true reality (universalism) or consists of multiple realities (relativism), how much of this reality is constituted by things (granular stocks or items) or by flows (processes), and how much of this reality is order or chaos, for example.

This study considers an ontology which is essentially the world of socio-technical systems. These systems are complex and composed of interactions between humans and technology, as well as between humans. These interactions can be synchronous (happening at the same time) or asynchronous (happening at different times) and can be geographically dispersed. The result of these interactions conditions and modifies the system itself, but results in an organization that functions due to the shared meanings and realities of all its members. This paradigm can be said to represent a subjectivist ontology, and more precisely, a social constructionist approach to knowledge. This assumption

considers that social reality is made of the perceptions and resulting actions of people (i.e., social actors). In particular, social-constructionism proposes that reality is established from social interactions, where the social actors present in the system create shared meanings and realities through repeated interactions. These shared meanings are also not static but are modified and evolve, according to feedback from the results of the flow of processes and interactions of the agents in the system. This is in contrast to a purely objectivist point of view, where there is a "truth" out there for which the research is said to be searching.

A subjectivist / social-constructionist research ontology reflects the role of the researcher as looking to describe the realities of the different members of an organization, looking to understand their incentives, actions and intentions. The representation of the different dimensions of organizational action is made explicitly through the use of System Dynamics, a methodology described in the next section.

A subjectivist /social constructionist approach also considers that the researcher not as an external, objective witness of what is being researched, but actively influencing these results. As such, known biases and assumptions have to be made public and presented explicitly to the research community.

The ontological approach adopted in this work assumes that events in the world are caused by behaviours or patterns, which in

turn are caused by the structures present in the system. However, these structures are too complex for understanding through intuition alone. Modelling thus becomes a way of representing these structures, reproducing the behaviours that are actually being seen, and simulate alternate behaviours by changing assumptions or structures.

3.3.2 Epistemological assumptions

Epistemology comes from the Latin "episteme" meaning "knowledge" and "logos" meaning "logical discourse", and the "epistemological position" of a research is a concept that describes the assumptions about what is constitutes meaningful knowledge, and how this knowledge is communicated to others. It refers to aspects such as "*how do we know what we know*", "*what can be considered as knowledge*", "*what constitutes good quality data*", and "*what types of contributions can be made to this knowledge pool*" (Sanders et al., 2016)

An epistemological position is thus defined in terms such as how the assumptions are adopted either from the natural sciences or the arts and humanities, how much of the information is considered as numbers or as narratives, how much of the information are facts or opinions, how much of what is to be analysed constitutes observable phenomena or are constituted by attributed meaning, and how much of the research outcomes are

law-like generalizations or highly context-and-individual specific, for example.

As an overarching review, and derived from the recognition that scientific knowledge is not absolute truth but a structured approximation to it, three main answers have been proposed to the question of "what is scientific knowledge". A first approach, supported by philosophers such as August Comte, considers scientific knowledge to be a tool that correlates data, a view known as Instrumentalism. Its advancement thus consists in the gathering of more and more data and /or by finding statistical fits to this data. A second view, advanced greatly by the philosopher Thomas Kuhn (1962), considers scientific knowledge as groups of ideas -known as paradigms- that help explain the world. In this second case, its advancement consists in the use of these paradigms on the data until unexplainable differences between the current paradigm and the data that is seen in the world require this paradigm to change. The third approach, advanced by the philosopher Karl Popper (1972) considers scientific knowledge to be a set of conjectures (i.e., opinions and conclusions based on incomplete information) that are refutable. In this case, the main method for advancement is the change or adjustment of conjectures to overcome these refutations, process known as "*refutationism*".

The epistemological approach that is taken in this work is the refutationist approach. Through this lens, no piece of knowledge is regarded as "valid", but rather as not having been yet refuted. Given the nascent nature of cyber-resilience in supply chains, the refutationist approach is seen as the most appropriate to accommodate new methodologies that do not rely exclusively on data or rely on data that is not quantitative and partial.

In order to define what is considered as knowledge within this research, it is important to also understand what is considered "scientific research" in the social sciences and particularly within this thesis. King et al. (1994) proposed a definition of scientific research that highlights four characteristics:

- First, *the goal of scientific research in the social sciences is an inference*, i.e., the generation of conclusions based on evidence and reasoning. This is achieved either through description or explanation, based on empirical information about the world. This discards the mere accumulation of facts as science in the social science realm, being rather that which can infer beyond the available data into something of wider scope that cannot necessarily be observed directly. Such non-immediate inferences include descriptive inference, i.e., from world observations learn about other facts that are not observed, and causal inference, i.e., the identification of temporal relationships between

observations, learning how one comes to pass because of the other,

- Second, *scientific procedures are public*, explicit and coded, providing a basis through which the data can be assessed, and its validity judged by the community to which the work is relevant. Establishing the procedures explicitly can help assess and address their limitations, and serve as a medium to teach and share these procedures, allowing for the replication and comparison of results across different disciplines and research projects,
- Third, *the conclusions of the scientific research are uncertain*, derived from the assumption that the inference process is imperfect, and that it is improbable that conclusions that are certain can be reached from uncertain data. It is therefore relevant to consider the uncertainty directly to avoid otherwise asserting that the scientist knows everything perfectly or that the scientist does not know about the uncertainty of the results, and
- Fourth, *the content of the scientific research is the method itself*, as it is the observance of these methods which help validate the results obtained in the research process. Since the subject matter that can be the subject of scientific research is so broad "*the unity of science consists alone in its method, not its material*" (Pearson, 1892, pp.15).

Therefore, scientific research does not need to be error free to be a contribution, as errors are unavoidable and when pointed out by others, highlight research as a social enterprise (King et al, 1994).

3.3.3 Axiological assumptions

Axiology comes from the Latin "*axia*" meaning "*value*" or "*worth*" and "*logos*" meaning "*logical discourse*". The axiological position of a research is the concept that represents the role of ethics and values in the research process. It deals with questions such as what is the role of values in research, how the researcher's values should be treated when performing the research, and how the values of the research participants should be considered.

An axiological position is thus a result of defining a stance in the trade-off between value-free and value-bound research, and between having a detached researcher and having a researcher that is an integral and reflexive part of the research.

The process of self-reflection by the researcher to understand the existing axiological standpoints cannot be overstated. The researcher's values are the basis upon which judgments are made during the research process, defines the way in which the research is originated, conditions how it subsequently evolves, (as the researcher normally includes his or her own positions into the

research project definition) and thus conditions the research action (King et al., 1994; Heron, 1996).

These positions include aspects such as any pre-existing assumptions about the problem and its contexts, interests of the researcher, or emotions associated with the research project. For example, having chosen this research topic over another is a reflection of the axiological position of the researcher, as the chosen topic is considered more important than other potential research topics. Therefore, having this position explicitly stated can only add to the credibility of the results.

3.3.3.1 Statement of personal values

My statement of personal values with respect to a research in the cyber-risks within global supply chains is based on the premise that supply chains are complex networks of interactions between humans and hardware, interactions which are enabled by a communication infrastructure that results in the physical movement and accumulation of goods, and the delivery of services. I believe supply chains to be some of the most impressive and important social structures created by mankind. Thus, the way in which modern supply chains can be disrupted can have not only commercial but also social implications, making research into the avoidance of, and recovery from disruptions to supply chains, of a high social relevance.

I believe organizations are the result of decisions that are made in people's heads, derived from the ideas they have about the systems and processes around them, in what can be termed as "mental models". I believe mental models to be a constituent part of how humans perceive and make sense of the world around them. However, I am also convinced that these mental models do not necessarily align with the existing systems where decisions are taken as these models may contain errors, or be crude simplifications of the real systems these decisions are set to manage. I believe that aligning those mental models with the actual system is the way of obtaining the greatest leverage differential result per unit effort (leverage) when considering change, yet it is a dimension of considerably more access difficulty than the traditional analysis of processes and organizational performance.

I believe that part of the "mental models" held by the decision makers are constituted by the incentives they see around them to the decisions they take. All sentient, biological creatures react to stimuli of which incentives are a particular kind. How much those actual incentives actually contribute to the ends sought by the company can be a source of misalignment between the goals of the company and decision-maker. This misalignment cannot be said to be the responsibility of the decision-maker, rather a problem in the design of the decision-making system within which the decision-maker is located. I, therefore, believe human error to

be an easy excuse for managers in what is really a design error of the system in which these humans work.

I believe managers really try to improve the systems they operate but have a lot going against them. As long as they concentrate on patching the behaviours, or blaming unwanted events and performance deficit on operator error, they are not really solving the problem, only buying time until the next unwanted event occurs. I also believe managers do not have the tools to understand the ways in which the systems they are set to manage to operate over time. The tools they have are largely static (by representing the state in one moment in time) while the systems are changing constantly. The tools they have are simplifications which despite having been used for simple systems, are increasingly unfit as the system complexity increases. The corporate pressures decision-makers face drive them towards short-term performance, while complex systems when intervened structurally for long-term improvement, normally present short-term decreased performance, which is difficult to justify without considering the long-term perspective.

I believe that addressing the deep structure of supply chains in search of the required behaviour is one of the duties of scientific research and that it is a significant potential contribution from academia to the industrial world: the possibility of looking at processes without the bias of corporate pressures for performance,

or optimum use of resources for short-term gains, is a differentiating advantage that allows academia to explore and propose beyond traditional paradigms.

3.3.4 Overall philosophy

The ontological, epistemological and axiological assumptions mentioned in the previous sections, can be summarized in a philosophical approach that can be better described as a mixture between critical realism and interpretivism, taking some aspects from each of these. The main aspects of each of these philosophies are explained next and contrasted with positivism, the philosophical approach most broadly found in scientific research.

Table 16 Research philosophies (Sanders et al., 2016)

	Positivism	Critical Realism	Interpretivism
Ontology (Nature of reality)	*Nature of being is real, external and independent *There is one true reality (Universalism), *Nature is ordered and granular/reducible	*The empirical, the actual and the real are layered, *External, independent and transient, *Objective structures, *Causal mechanisms.	*Complex and rich empirical, actual and real constructs, *Socially constructed through culture and language, *Multiple meanings, interpretation and realities, *Flux of processes, experiences and practices
Epistemology (What constitutes acceptable knowledge)	*Use of the scientific method, *Observable and measurable facts, *Law-Like generalizations, *Causal explanation and prediction as contribution.	*Epistemological relativism, *Knowledge historically situated and transient, *Facts are social constructions, *Historical causal explanation as contribution.	*Focuses on Narratives, stories, perceptions and interpretations, *New understandings and worldviews as contribution.
Axiology (The role of values)	*Value-free research, *Researcher is detached, neutral and Independent of what is being researched, *Researcher maintains objective stance	*Value-laden research, *Researcher acknowledges bias by world-views, cultural experience and upbringing, *Researcher tries to minimize bias and errors, *Researcher is as objective as possible.	*Value-bound research, *Researchers are part of what is researched, *Research is subjective, interpretations are key to contribution, *Researcher is reflexive.

3.3.5 Challenges with the systems approach

The validation of models and the information that can be obtained from them has been subject of analysis and critique by philosophers of science. The challenges that have been identified can be classified as ontological, epistemological and methodological in nature.

The ontological challenge of using SD models for scientific research is embodied in that, despite their instrumental value, a sense needs to be defined in which SD model structures exist objectively in reality. To address this challenge, SD model can be said to be of ontological value by assuming that the structures proposed in the models represent something objectively real, since these models make explicit something that exists in the social world. The social world is interpreted by us in specific ways through which we give structure to reality. Therefore these constructions as represented in the SD models, can be as real as any of our intentional constructions. As such this is rooted deep in the idealist/presentationalist philosophy.

The epistemological challenge of using SD models for scientific research is embodied in that, despite the explicit structure of SD models, a definition is needed of how SD models can have any explanatory value. This is, even if the causal relationships between the components of the system do have explanatory value, a sense needs to be defined in which these

relationships deliver genuine causal explanations. To address this challenge, it can be understood that SD models represent in explicit terms the knowledge contained implicitly in the actions of the agents involved in the system that is being modeled. SD models then reflect the consequences of these structures. Explanations that come from these structures reveal therefore what is implicit in the actions of the agents involved in the modeled systems.

The methodological challenge in using SD Models refers to how system dynamics models can help create well-founded theories about the phenomena that are modelled. To address this challenge, it can be understood that SD Models reflect relationships between constructs present in the system that is modelled. As such, these relationships also represent logical relationships that explicit the inferences that are implicit in our discursive practices. Logical relationships that present a constancy across system representations of different members and agent in the system can be understood as logical truths, which in turn help us identify inferential constants in our discursive practices.

This is by no means a settled matter, as the philosophical implications to science of using System Dynamics Models for scientific advancement is being researched from the point of view of its philosophical background. Examples of this include Barlas, 1996; Vasquez et al., 2007; and Olaya, 2009.

3.4 Research approach to theory development

Once a philosophical position has been chosen for the research, it is necessary to identify and define the research approach to theory development, in what is also called the research "*logic*" (Saunders et al., 2016). The research approach represents the process through which theory is advanced, and thus the way in which knowledge is produced.

The starting point of a research could be an existing theory and the research process, through data gathering arrives at logical conclusions about this theory, process defined as "deductive". It may also be that observations from the world are surprising with respect to an existing theory and the research, through data gathering, helps in refining that theory, a process known as "abductive" or "retroductive". Finally, there may be no specific pre-existing theoretical framework to start with, and the research process converts data from the world into a proposed theory, process known as inductive. Sanders (2016) presents a summary of these features as shown in Table 17.

Table 17 Inference strategy comparison (Sanders et al., 2016)

	Deduction (Deductive Inference)	Induction (Inductive Inference)	Abduction (Abductive Inference)
Logic (Relationship between Premises and Conclusion	If the premises are true then the conclusion must also be true	Known premises are used to construct untested conclusions	Known premises are used to generate testeable conclusions
Generalisability (Relationship between the Specific and the general)	Generalises from the general to the specific	Generalises from the specific to the general	Generalises from interactions between the specific and the general
Use of Data Collection	Data used to test (evaluate) hypothesis regarding an existing theory	Data used to explore a phenomenon, indentify patterns and themes, to create a conceptual framework	Data used to explore a phenomenon, patterns, and themes within an existing conceptual framework, and then test this
Theory (How theory is advanced)	Theory falsification or verification	Theory generation and buiilding	Theory generation or modification

The process for each of these types of inference requires an interaction between the framework that is used to understand reality (theoretical position) and the information obtained from the world (empirical position), a process that has been explored by Chris Voss and his team at Warwick Business School. Voss (2015) summarizes it in flow diagrams shown in Figure 26.

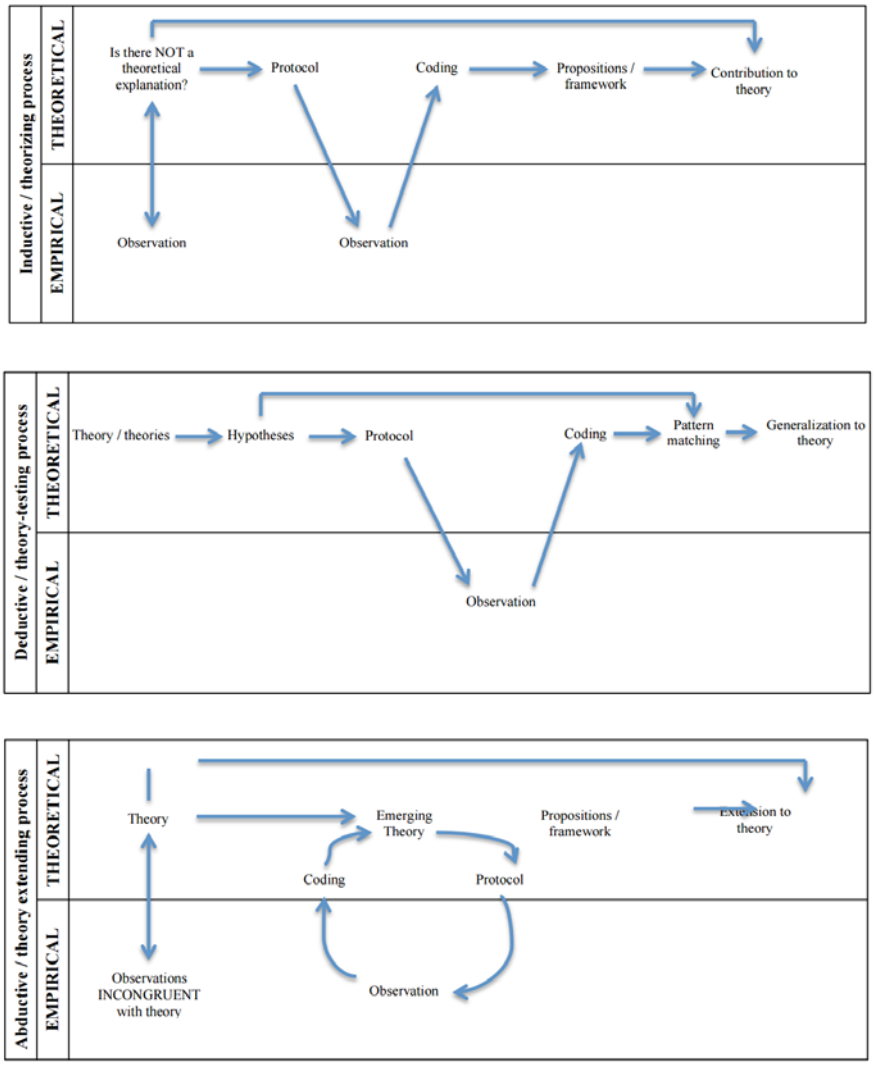

Figure 26 Theory Development vs. Inference (Voss et al., 2015)

Voss argues that the interaction between the theoretical and empirical dimensions happens in different moments of the process, according to the theory development approach that is chosen. For both the deductive and abductive approaches, there is a starting theoretical framework. Either hypotheses derived from

this framework are proven/disproven (deductive approach), or incongruences between the theoretical framework and observations in the real world lead to theory extensions (abductive approach). In contrast, the inductive approach does not start with an existing theoretical framework for a current observation from the world and therefore requires a protocol to gather information in a structured way for the identification of patterns and subsequent theory creation through the generalization of these patterns.

These processes of inductive and abductive inference can also be understood from a systems perspective as attempting to converge the ideas currently accepted about the underlying system structure that leads to the system behaviour and then to the actual observed behaviour from that system. The "*systems approach to inference*" is a central part of the methods and tools proposed and used in this thesis.

In the metaphor of the iceberg, if the system behaviour is what is observable (e.g., above the water) then the patterns that lead to that behaviour, the accepted ideas about system structure that leads to those patterns of behaviour, and the mental models that result in those ideas about the system structures, is what is hidden below the water, as can be seen in Figure 27.

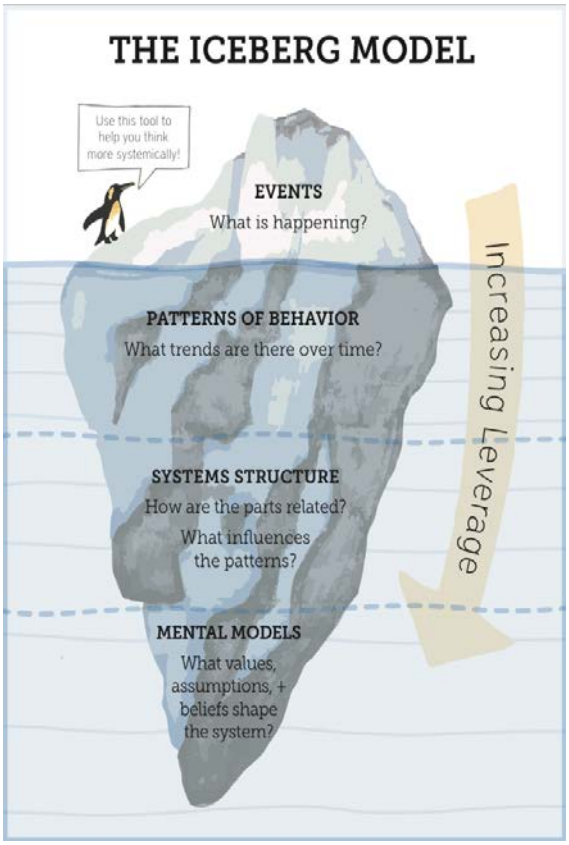

Figure 27 Iceberg metaphor

In this analogy, for the inductive method, the system structure is not known as it is hidden from view. For the abductive method, a structure can be extracted from the people in the system, so it is visible, but its validity is not clear. The research process seeks to increasingly understand this structure by continually improving it through subsequent approximations of ideas about that structure, ideas that become better with more data about the actual behaviour of the system, this is what can be observable, and through testing

the ideas that people with knowledge about the system have about its structure.

This approach recalls the allegory of the cave by Plato as laid out in “the Republic” (Annas, 1981), which describes the dialogue between Socrates and Plato’s brother Glaucon, who was being mentored by Socrates. In this allegory, Socrates tells the story of a group of men that were prisoners in a cave unable to turn their heads. All they can see is the wall of the cave. To their back there burned a fire and in between the prisoners and the fire, there were puppeteers. Thus, the prisoners were only able to look at the shadow cast by these puppets, not the real objects.

One first insight given by Socrates is that these prisoners may mistake appearance for reality, thinking that the shadow is the truth, although they would know nothing about the causes of the shadow. In the same logic, a researcher observing a system may think they understand the system by looking at its behaviour, although they know nothing about the system structures that lead to that behaviour.

The second insight is that only when the prisoners turn their heads and see the source of the shadows, do they realize their mistake. In the same way, only by looking at the structure (i.e., the proverbial turning of the head) would a researcher realize the source of the behaviour.

A third insight is that the perceptual experience of the shadows only provides a one manifestation of potentially many about an underlying structure and in no way defines it: in the same way that the shadow does not define the fire-puppet arrangement but is instead caused by it, perception of system behaviour does not define the system causing the behaviour and is merely one of many possible manifestations given the system structure. This notion of causality is central to the choice of methodology and is discussed in the next section.

Still connected to the iceberg model, an initial idea of the structure behind a behaviour of interest, derives into hypotheses about this or other interesting behaviours of the system, hypotheses that are proved or disproved through data. This would be the deductive case.

Incoherence can emerge when a prior idea about the structure behind a behaviour of interest, contradicts the observation of a different behaviour than what was expected according to the original idea of the system structure. This incoherence motivates the gathering of data to adjust this perceived system structure so that it approximates better to the observed behaviour of interest. This would be the abductive case. If on the other hand, no specific underlying structure is considered as resulting in an observed behaviour of interest, the gathering of data is used to propose a

structure behind a this system behaviour. This is the inductive approach.

A deductive approach uses the accepted idea about a system's structure to prove and disprove hypotheses about the behaviour of that system. The iterative process is therefore at the level of the events and no update of the idea of the structure takes place. The abductive approach uses the accepted idea of a system's structure and its incoherence with an observed behaviour, to update this held idea about the system's structure. The inductive approach starts at the level of observed behaviours and attempts to propose an idea of a structure that would result in those observed behaviours.

From this conceptualization of theory building, it is also possible to identify relationships between these inference strategies. For example, an abductive process is likely to happen after an inductive process, since only once observations about the real world have been translated into an idea of a structure that causes these observations, can incoherent observations be used for theory development. Also, abductive processes do not seem to derive from deductive processes, as these do not question the underlying structure: process would rather declare a hypothesis as false rather than question if the hypothesis was sensible (justifiable due to the underlying structure) in the first place. This is one of the main critiques put forward to positivist approaches to

research, as these tend to encase research within an artificially tight theoretical framework, discarding dissonant observations as extremes or anomalies (Boer et al, 2016, Sanders et al., 2016).

Time availability is an aspect to consider with regard to the inference approach that is to be followed. Deductive inference is typically quicker to complete than inductive or abductive approaches. Deductive research is based on a one-time data gathering and a predetermined framework through which this data is to be analysed and the hypotheses tested, while the inductive and abductive approaches require an iterative data gathering process, and the gradual identification of frameworks.

Risk aversion is also important at the time of deciding the strategy to follow, as the inductive and abductive research types are normally riskier as it is always possible in these that no useful patterns or theory emerges.

The topic of cyber-risk and resilience in the global supply chain does not have a formal existing framework that explains the nature of cyber-risks, the structure that leads to effective cyber-risk management or the structure that leads to resilient behaviour. Therefore it would not be credible to use either the deductive approach for any of those case.

According to the results from the SLR, for understanding the nature of cyber-risks, data has to be gathered from alternate data sources. Without a pre-defined framework to understand this

nature of cyber-risks, this process is considered as an inductive approach.

Yet, since "*we all create and update cognitive maps of causal connections*" (Sterman, 2000, p.28) people that are knowledgeable about the system have an idea of the structure behind the behaviour that is observed. When the structure that different people have about the same system is compared and agreed upon, a resulting model can be tested against actual behavioural data.

As the structures that are revealed from the interviews reflect a structure that understands the world, both the risk analysis and the dynamic analysis for the research in this thesis follows an inductive approach.

This is consistent with the approach that has been followed in the social sciences and contrasts with a deductive approach which has been mainly used in the natural sciences.

Despite the increased risk profile of the inductive research approach, this was chosen to understand the nature of cyber-risks, as few relevant frameworks for this end were found through the literature review.

3.5 Research strategy/design background

Once the strategic aspects underlying the research process have been defined, the research strategy, also known as the research

design, has to be determined. The design corresponds to how the specific research is to be carried out and is concerned with techniques and procedures that researchers use to gather and analyse data (Grix, 2002). Once the epistemological position of the research defines what is considered knowledge for the research process, the method chosen determines how this knowledge can be acquired, without yet identifying the precise procedures. The method that is chosen is independent of, and unconstrained from the epistemological choice (i.e., what the researcher thinks can be researched) and is rather influenced by the research questions.

This research design is determined by the research method, the research purpose and the methodological choice.

3.5.1 Research method

Method is derived from the Greek μέθοδος [methodos], meaning "*pursuit of knowledge*" and is distinct from the methodology: while the latter deals with the system that is considered for the research, including philosophical position, logic, strategy and design, the former is concerned with the procedures and techniques used in the research to gather and analyse data (Grix, 2002). To avoid this misunderstanding, Sanders et al. (2016) rather use the term *research strategy* when referring to the method that is used, as it can be seen from the research onion in Figure 20.

The methods available range from mainly qualitative to mainly quantitative, and can be classified as allowing research that is descriptive, explanatory, and evaluative or a combination of these.

The *experiment* as a research strategy has its foundation in the natural sciences, and it has been widely used in psychological and social science research. The purpose of an experiment is to deliberately manipulate a variable, called "*independent variable*", to study what the outcome is in another variable, called the "*dependent variable*". By using a set of predictions of this outcome, known as "*hypotheses*" (equivalent to a pre-existing framework to be tested, and is thus a deductive inference approach) the result of the experiment being either that there is no significant relationship between the dependent and the independent variable, prediction known as "*null hypothesis*", or there is a significant relationship between the independent and the dependent variable, prediction known as "*alternative hypothesis*". This can be tested statistically and although the basic experiment tests the relationship between two variables, it can be complemented by the use of other variables concerning the problem, such as moderator variables which affect the nature of the relationship between the dependent and the independent variable, or control variables, i.e., those observable and measurable variables that need to be kept constant throughout the experiment, to limit the influence of the relationship between the dependent and independent variable.

The *survey* as a research strategy is normally associated with the deductive inference approach is used for descriptive or exploratory research. A survey using questionnaires allows for the collection of data that can be analysed quantitatively through descriptive and inferential statistics. Additional to a questionnaire, other methods of gathering data include structured observation and structured interviews.

An *archival and documentary research* is the collection of data through historical data. Despite it being difficult to completely define all the potential sources of historical data, it has been suggested that a document is "*a durable repository for textual, visual and audio representations*" (Sanders et al., 2016). Some of the documents categories are used include:

- Communication records such as emails, letters, social media or blog postings;
- Individual records such as diaries or electronic calendars;
- Organizational records, such as agendas, meeting minutes, agreements, contracts, reports or strategy documents;
- Governmental records, such as national statistics or reports;
- Media sources, such as printed and online articles.

Since the records being used for this method were not originally created for the research, but rather gathered through it, is that they are considered as secondary data.

A *case study* research seeks to make an "*in-depth inquiry into a topic or a phenomenon within its real-life setting*" (Yin, 1994). The unit of analysis is identified, as it might be a person, an organization or an event, for example. Then the relationships between the case subject and its context are described and analysed. The case study is useful in instances when the boundaries between the subject and the context are not clear, and it can lead to rich empirical descriptions, and to the development of theory. There is no precise way to carry out a case study as it has been used both by positivist as well as interpretivist researchers, and case study has been used for exploratory, descriptive and explanatory research. Yin (1994) has distinguished two dimensions along which a case study can be defined: single versus multiple cases, and holistic versus embedded cases, the latter of the dimensions relating to the unit of analysis, i.e., a whole organization (holistic) or specific departments (embedded).

An *ethnographic research* is used to gather data about behavioural patterns between members of a particular group, thus having particular use in studies about culture and society. It is a strategy that has its origins in colonial anthropology (Sanders et al., 2016) and is normally done over extended periods of time,i.e., "*longitudinal research*". This is in contrast to "*transversal research*" which is normally shorter as evolution over time is not a factor.

Action research is a process followed iteratively to develop solutions in organizations through collaboration and participation of the organization itself. Its strategy is to "*promote organizational learning to produce practical outcomes through identifying issues, planning action, taking action and evaluating action*" (Sanders et al., 2016) having been described as "*research in action rather than research about action*" (Coghlan et al., 2014).

Grounded theory research is an approach to theory building by using inductive and deductive approaches, and is a process to analyse, interpret and explain the meanings that the members of an organization build to make sense of their collective experience, through the building of theoretical explanations of social interactions. By providing a systematic approach to data collection and analysis, the grounded theory provides a framework to undertake qualitative research (Sanders et al., 2016). Despite being catalogued as a mixture of inductive and deductive approaches, it has been argued that it might be more appropriate to think of it as abductive (Suddaby, 2006). The data that is collected through this research strategy is not indicated by the method, and therefore, the grounded theory can be based on different forms of data collection approaches. Grounded theory research is generally considered to be time consuming, and longitudinal in its approach, i.e., it extends the research and data gathering collection over periods of time, despite the time factor

not necessarily being part of the final theoretical framework that is achieved.

A *narrative enquiry* research is a strategy that uses a story, (personal account) to interpret an event or a sequence of events, particularly seeking to record the chronological connections and the sequence of events as told by the participant (narrator), their interpretation of events, and the potential triangulation of narratives between different participants and their narratives about a common event or sequence of events (Chase, 2011). This strategy has been associated with small samples with specific purpose and objectives, as it is a time-consuming approach, normally generating large quantities of qualitative data that require special coding approaches such as structural narrative analysis (Sanders et al., 2016).

Simulation-based research is an approach beyond the traditional research strategies mentioned so far, and despite being a method that has been advanced in engineering, it has so far had limited penetration in the social sciences. It is a method through which a researcher develops a representation of a phenomenon under investigation, i.e., the model, and chooses a simulation method that is coded into computer software. This model is then "*run*" many times under different conditions as necessary, to observe and analyse the outcomes from where to advance theory. It is reported that an average of 8% of the published articles over

the period 1994-2003 in social science journals used simulation as a tool for theory development, with numbers for operations management as low as 0.3% for the Academy of Management Journal, and as high as high as 24% for Management Science Journal (Harrison et al., 2007). Simulation has several advantages with respect to other research strategies, as it allows for the exploration of the interdependent behaviour of phenomena that individually may be well understood, but which might have complicated and unforeseen interactions. Meadows and her team mentioned some of the advantages related to the simulation of models as: their rigorousness through explicit specification, their comprehensiveness through their ability to process great amounts of information, their logic through a visible outcome from a set of assumptions, their accessibility through explicit, precise and unambiguous assumptions, and their flexibility through the possibility of repeated testing under a wide range of conditions (Meadows et al., 1985). Simulation is strongest for understanding a phenomenon for the purposes of behaviour prediction, as "*proof of behavior*" to test if a certain behaviour is even possible, for discovery of unexpected consequences, for explaining underlying processes behind observed behaviours, as a tool to criticize pre-existing explanations of phenomena to find simpler explanations, for prescribing better ways of performing a process, as a tool for formalizing theory, and is particularly well suited for dealing with non-linear phenomena (Axelrod, 1997; Gilbert, 2005; Harrison et

al., 2007). Some of the risks and disadvantages of simulation is model misspecification, the technical difficulties of model development, problem of generalization beyond the specific parameters of the model, and particularly an insufficient understanding of the methods by the business and social science research community for them to be considered as a plausible research strategy (Harrison et al., 2007). For example, Sanders et al. (2016) in the latest edition of the book "*Research methods for business students*" does not once mention simulation as an available tool for social science research in business, despite this method being around for over 50 years (Forrester, 1961; Cohen et al., 1965). Some types of possible simulation methods are agent-based modelling, system dynamics modelling, econometric modelling, and discrete event simulation, for example.

3.5.2 Research purpose

In order to identify the suitable research design, it is important to identify the purpose that this research design is pursuing. Sanders et al., (2016) propose a number of research purposes, namely exploratory, descriptive, explanatory, evaluative or any combination of these.

- An *exploratory research* is directed towards the opening and gaining insights about an area of interest. The associated research questions are likely to start with "what" and "how", and it is a research purpose that might throw

light on the feasibility of continuing to research some particular subject area. For this reason, it is a flexible research purpose that by its nature, adapts to the data that is being gathered.

- A *descriptive research* wants to result in an accurate representation of a phenomenon, and are likely to have research questions that start with words such as “who”, “what”, “where”, “when” or “how”. It is not normally used as an end, but a way towards explaining the phenomenon beyond its mere description, and is thus considered a precursor to an explanatory study.
- An *explanatory research* is looking to identify causal relationships between variables to answer questions intended to explain a phenomenon. Associated research questions are likely to start with or include “why” and “how” in their formulation.
- An *evaluative research* is intended to identify how well something works, and thus its results evaluate research questions that are likely to start or include “how”, “what” and “to what extent”. This purpose is directed towards assessing effectiveness, making comparisons, and thus its theoretical contribution is not only understanding how the effectiveness is reached but why, to then compare this explanation to existing theory.

3.5.3 Methodological choice

With the consideration of possible exploratory, descriptive, explanatory and evaluative research purposes for this research, it is also important to identify and define the methodological choices available for a research, in terms of three dimensions: quantitative versus qualitative, multi versus mono-method, and simple versus complex/mixed methods.

A *quantitative research* is generally associated with positivism, and thus it is associated with the deductive approach to theory development, where the focus is to use data to test the theory. A quantitative approach has also been used to use data to develop theory. As such, a quantitative approach seeks to identify and analyse relationships between variables by different numerical and graphical methods. It can thus be used either from data coming from a single or multiple data collection techniques.

On the other hand, *qualitative research* is rather associated with some philosophy that requires the interpretation of the data that is gathered, and where the focus is to build theory or to develop a modified theoretical framework than the one currently being used. Yin (1994) suggested, however, the use of qualitative research for a deductive approach to test certain theory through qualitative means. In practice, however, quantitative approaches are used more widely in processes of inductive or abductive inference. The data that is collected is not standardized, and some methods may

even consider information that emerges from the data gathering process (e.g., conversations leading to new questions not considered originally). Qualitative studies can also consider one or multiple methods for the data collection and analysis.

In contrast with the *mono- versus multi-method* which is the determination of the number of data collection techniques that are going to be used in the research for either the quantitative or the qualitative research designs.

The use of one or both qualitative and quantitative methods is the research design position that is known as *simple versus mixed methods* respectively.

3.6 Research design overview

In order to identify the appropriate research design, the research sub-questions that were identified after the systematic literature review were evaluated from the point of view of the purpose of the research. After careful evaluation, and as it is explained in this section, this research is a combination of the exploratory, descriptive, explanatory and evaluative purposes.

For the case of RSQ3, as the problem of cyber-attacks and their effects in supply chains is still poorly understood, the first research question is related to identifying the particular characteristics of these risks and of how these differ from other supply chain risks. This research question has been divided into

three sub-questions. First, this thesis undertakes an exploratory approach for identifying what events of operational disruption caused by cyber-risks have been recorded, the topic of RSQ3.1. This differs from the RSQ2, as that question only took into consideration those events that had been published. The difference is not trivial, as the results of RSQ2 revealed only a few published cases. Answering RSQ3.1, therefore, requires looking an exploration into other sources of information about cyber-attacks beyond published literature.

With the information retrieved from RSQ3.1, the next two sub-questions are answered: first by using this information to describe the mechanisms through which a disruption is caused (descriptive purpose) originating RSQ3.2, and then by comparing these mechanisms with those caused by other supply chain risks (evaluative purpose), covered by RSQ3.3.

In the case of RSQ4, the management of cyber-risk and resilience is separated into two parts, 1) the management of cyber-risk and 2) the management of cyber-resilience, considering methods based on systems thinking for application to each part. As a result, two approaches rooted in systems thinking and successfully used in other knowledge domains, are identified, implemented and tested for the case of cyber-risks: first a method of systemic risk analysis and second a method of dynamic

simulation, both methods applied to cases of cyber-attacks focused on the operational disruption these attacks cause.

Additionally, the research sub-question 4.1 related to the application of a systemic risk analysis, this is separated in two parts to

- First address how a systemic risk analysis method addresses the method-related gaps identified in the SLR, i.e., compartmentalization, static vs. dynamic, and history-dependency, and
- Second, address the suitability of such a method by comparing it to some other established risk analysis method applied to the analysis of cyber risks. The purpose of each research sub-question is detailed in Table 18.

Table 18 Purpose of research for each research sub-question

Research question		Exploratory	Descriptive	Explanatory	Evaluative
RSQ3	**How do cyber risks cause operational disruption in supply chains, and how does this differ from other supply chain risks?**	RSQ3.1.-What events of operational disruption caused by cyber risks have been recorded?	RSQ3.2.- How have these events resulted in operational disruption?		RSQ3.3. - How do events from cyber risks differ from events from other supply chain risks?
RSQ4	**How can a systems approach be used to mitigate compartmentalization, static frameworks and historical-dependence for managing cyber risks in the supply chain?**			RSQ4.1a. - How can a systemic risk analysis approach mitigate compartmentalization, static frameworks and historical dependence for managing cyber risks in the supply chain?	RSQ4.1b. - How does a systemic risk analysis approach compare to established risk analysis methods?
				RSQ4.2. - How can System Dynamics simulation mitigate compartmentalization, static frameworks and historical dependence for managing cyber risks in the supply chain?	

The data types that are needed for researching each of these questions is

3.7 Research design - The nature of cyber-risks

Answering RSQ3 requires information from other data sources beyond published literature to obtain information. Therefore answering RSQ3 requires finding out which other information sources are available for data about cyber-attacks with operational disruption. Moreover, as these sources consider literature beyond published, peer-reviewed articles (as these were already addressed during the literature review), there is the matter of the validity of these new sources, in a trade-off between the need for updated information versus the validity of the information that is used to derive scientific insights.

Not being the only possible approach, the strategy undertaken for this part of the research is one of archival and documentary research, with a focus on the review of news articles and reports.

The research is not intended to be exhaustive. Rather, a revelatory search is sufficient to uncover the characteristics and attack mechanics required to answer research questions 3.1 to 3.3.

3.7.1 Data sources

This part of the research uses secondary data. The data sources are obtained through an archival and documentary research strategy, to review documentary accounts of cyber-attacks

publicly available. For this search was carried out through internet search engines to establish where these accounts of cyber-attacks were being published online. Through this method, a raw database is extracted for analysis. The research protocol is:

- The online databases used are:
    - Newspaperarchieve.com, a subscription database with search engine accessed through MIT Library (http://libraries.mit.edu/) during the period November 2016 to May 2017.
    - Googles news, an open-access database, http://news.google.com
    - ProQuest news and newspapers, an online subscription database located at http://www.proquest.com/libraries/academic/news-newspapers/, accessed through the MIT Library (http://libraries.mit.edu/) during the period November 2016 to May 2017.
- The data is obtained through the use of keywords “cyber-attack”, “cyber-risk”, “hacker” and “Information disruption”, and the search timeframe considered current news to this PhD project timeframe from November 2014 to May 2017.
- The filter for the validity of sources is: documents are included when these have an origin in an established

newspaper with regional or national circulation, cyber-attack research institutes, hardware or software manufacturers, cyber-attack specialists that have been referenced in established newspapers, government agencies, and universities.

- The filter for the validity of content is: documents are included when these describe a cyber-attack that resulted in operational disruption.

The protocol is laid out in Table 19.

Table 19 Research protocol for the nature of cyber-risks

Relevant Theoretical frameworks SLR	Archival and Documentary research
Context for research	Cyber attacks continue to occur in suply chains. Yet, it is not clear how these risks occur or how they differ from other risks in the supply chain. If these differ, then new options of management might be necessary.
Unit of Analysis	1.- News articles 2.- Reports by International organizations, agencies and consultants 3.- Newsletters dealing with cyber attacks
Research Question	RSQ3: how do cyber risks cause operational disruption in supply chains and how does this differ from other supply chain risks?
Sources of Data	• Newspaperarchieve.com, a subscription database with search engine accessed through MIT Library (http://libraries.mit.edu/) during the period November 2016 to May 2017. • Google.com, an open-access database • Proquest news and newspapers, an online subscription database located at http://www.proquest.com/libraries/academic/news-newspapers/, accessed through the MIT Library (http://libraries.mit.edu/) during the period November 2016 to May 2017.
Keyword combinations	(“cyber-attack” OR “cyber-risk” OR “hacker”) AND (“Information disruption” OR "disruption")
Search Strategy	1.- Use selected "Search Engines" with the "Keyword combinations" to obtain a first selection of documents. 2.- Review and filter documents according to the validity of sources criteria. 3.- Revire and filter documents according to the validity of content criteria.

Validity of sources	*Established Newspaper of regional or national circulation, cyber-attack research institutes, hardware and software manufacturers, cyber-attack specialists that have been referenced in established newspapers, government agencies, and universities (Technical Competence of author)
Validity of content	*documents describe a cyber-attack that resulted in operational disruption

3.7.2 Data analysis

The gathered information is analysed sequentially according to 1) a general description of the event 2) the structure of the case also called the "*physics*" of the case, 3) the patterns that result from the case structures described in each report, and 4) the differences these patterns present to other supply chain risks.

The *physics* of the case refers to the series of events and agents involved in a particular event (Sterman, 2000). In this case, the event is operational disruption resulting from a cyber-attack. From the systems thinking position, this analysis identifies the structures involved in the cyber-attack becoming the unwanted event. The result of this part of the analysis is 1) descriptions of cyber-attacks with operational disruptions, and 2) indication of the attack structure, i.e., agents involved including the external hacker and communications between the agents and with the environment.

During the analysis of the case structures, patterns for the disruptions are identified and categorized. According to the systems thinking position, the categories are identified as relating to some aspect of a common structure such as agents or communication patterns involved.

Finally, the patterns and categories identified from the cases are compared to other supply chain risks to identify defining characteristics, i.e., the "*nature*", of supply chain cyber risks. The next section will describe a small discussion about the supply chain risk categories to identify those with which cyber-risks are compared.

3.7.3 Supply chain risk source categories

Multiple categorization frameworks for risk sources have been proposed in the literature and by industry. Christopher identifies supply chain risks as originating in one of five possible "*sources*": 1) supply risks, 2) process risks, 3) demand risks, 4) control risks, and 5) environmental risks (Christopher, 2011, p.195).

Despite being exhaustive, these categories for sources of risk are not exclusive, leading to problems in their application. For example, the case of a flood can at the simultaneously originate demand, supply, process, and control risks. The "*sources*" as per Christopher are thus more accurately "*areas*" of risk which might have a source in the area itself or elsewhere. Christopher makes

no mention of cyber risks within any of the categories. Being embedded in different categories in the framework, it is therefore unclear how cyber-risks can be compared to any of these categories.

Sheffi proposes a "*dichotomy*" (Sheffi, 2015) of risks to supply chains as originating from one of nine sources: 1) competition risks, 2) economy risks, 3) accidents, 4) government and politics, 5) social discontent, 6) non-compliance, 7) intentional disruptions, 8) supplier failure, and 9) random phenomena. Sheffi derives these sources from cases of supply chain disruptions. However, these categories mix a series of concepts such as 1) motives, e.g., "*social discontent*", 2) normal market operating conditions, e.g., "*competition risks*" or "*non-compliance*", and 3) environmental conditions out of control, e.g., "*economy risks*" or "*government and politics*", "*random phenomena*".

Moreover, the category of "*intentional risks*" is misleading, since if it is assumed that the categories are exclusive, the "*intentional risk*" category would imply that all other categories are unintentional, which is not the case. For example, competition risk in the form of artificially low market prices can be generated as a way of purposefully affecting other companies in the market, making it an intentional source, which manifests through competition risk.

Sheffi's approach to supply chain risk categorization considers cyber-risks as part of the "*intentional risk*" category. In the same way as the example of the purposeful competition risk example above, this categorization is misleading. For example, cyber-risks can generate supplier failure risks, lead to non-compliance or be accidental instead of intentional. As a result, cyber-risks can be compared only to some of the risk categories in the framework proposed by Sheffi.

DHL proposes a categorization of supply chain risks according to four main sources (DHL, 2015), 1) *operational risks*, composed of IT failure, supplier failure, cargo problems and infrastructure problems, 2) *natural disaster risk*, composed of earth, wind, fire, and water origins, 3) *transportation risks*, composed of ground, marine and aviation sources, and 4) *socio-political risks*, composed of security, political violence or strikes. This categorization is illustrated in Figure 28, which shows examples of triggers that create a disruption through these risks.

Within each of the four categories the sources can be multiple, e.g., security and political violence can occur simultaneously, or IT failure and cargo problems can occur at the same time, and there is a distinction between categories which is useful for a comparison with cyber risks as a source of disruption, considered in the DHL framework (DHL, 2015) as all risks except IT Failure.

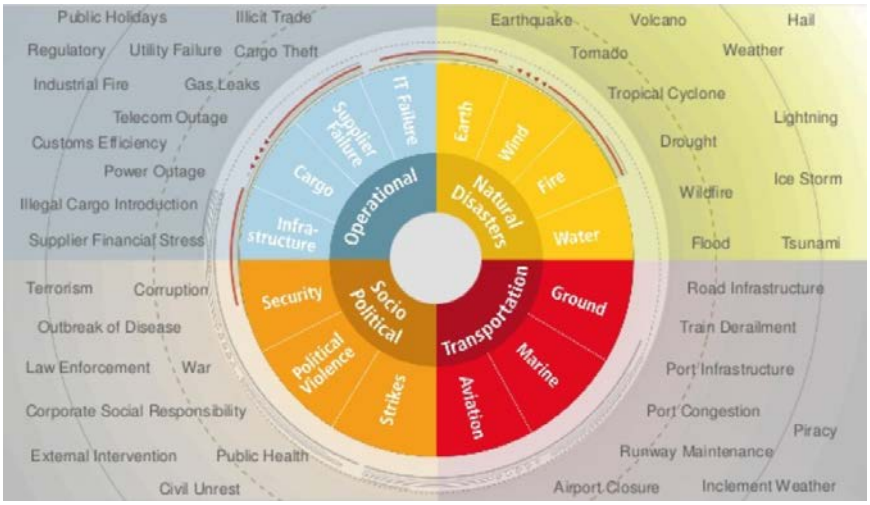

Figure 28 DHL Resilience360 risk categories (DHL, 2015)

The general model of disruption that is followed, according to the systems thinking framework, is a sequence of 1) a risk source leading to 2) the exploitation of a supply chain vulnerability that leads to 3) the manifestation of a disruption. This equivalent to 1) a structure, i.e., a risk source activating a vulnerability, that leads to 2) a pattern, i.e., the exploitation of a vulnerability, which results in 3) a behaviour, i.e., the manifestation of a vulnerability. This sequence is the basis of systems thinking as is represented in Figure 27.

Once the vulnerability is exploited the effects depend on the vulnerability itself, irrespective of the source that caused the exploitation. As a result, the comparison between cyber-risks and other supply chain risks is bounded to how the risk source exploits a vulnerability.

Consider the following example. An earthquake might result in a road being unavailable for delivery routing due to some physical obstruction or its destruction. In the same way, a cyber-risk might lead to a cyber-attack that deletes paths on the GPS system making these paths unavailable for delivery routing. A vulnerability of a supply chain might be the lack of adaptive routing for dealing with cases of path unavailability. The effect is a delayed delivery to customers or no delivery at all.

The comparison in this research is related to how the sources, i.e., an earthquake versus a cyber-attack, exploit the existing vulnerability, i.e., the lack of an adaptive routing system, rather than how this lack of adaptive routing affects delivery performance.

Cyber-risks are compared to 1) other operational risks, 2) natural disasters, 3) transportation risks, and 4) socio-political risks to identify unique cyber-risk characteristics.

Furthermore, cyber-risks are compared to the natural disaster risk in terms of how the source exploits the vulnerability. Examples of this comparison are a proposal from this thesis and run along dimensions such as:

- *Latency*: refers to the period between occurrence and discovery of a disruption from the risk. High latency means a long time between occurrence and discovery.

- *Physical location*: refers to the geography where the disruption from the risk is manifested, ranging from localized to un-localized.
- *Complexity*: refers to the number of agents in the supply chain affected by a disruption from the risk.
- *Replication*: refers to the way in which the disruption can continue occurring in other parts of the supply network.
- *Perpetuity*: refers to the effect over time of the disruption from the risk.
- *Component versus interaction risk*: refers to the type of failure causing the disruption from the risk.
- *Anonymity*: refers to the information about the controller, if any, originating the disruption from the risk.

3.8 Research design – Systemic risk analysis

This section presents a justification for the choice of a systemic risk analysis to answer the research sub-question 4.1, and it describes the data gathering process, and the case selection, to end with a mention of the software that was used.

3.8.1 Why a systemic risk analysis

All risk analysis methods to some extent relate to a more generic process of identifying, quantifying and reducing risk (Frosdick, 1997; Khan et al., 2007), and traditional approaches have followed the "*analytical reduction*" method of separating a

problem into smaller subunits, understanding the behaviour of each unit separately and then integrating this understanding into an understanding of the whole.

Traditional notions of risk consider it to be the probability of failure of a system, as derived from two characteristics of the system, the probability of occurrence of a specific mode of failure that leads to an unwanted event, and the consequence or severity of the failure mode materializing. These ways in which the mode of failure can materialize have been identified normally through methods such as fault tree analysis, event tree analysis, the HAZard and OPerability analysis (HAZOP), and the Failure Mode and Effects Analysis (FMEA). These methods link a cause with an undesirable effect, but "*are unable to include aspects such as design errors, such as software flaws, component interaction accidents, cognitively complex human decision-making errors, and social, organizational and management factors contributing to an unwanted event*" (Leveson, 2011, p.211).

In contrast, a systemic approach is based on two different set of ideas which characterize systems: emergence and hierarchy, and communication and control (see section 3.2.1). These concepts introduce ideas that would be invisible through analytic reduction approaches, such as coordination failure through system flaws, that is, undesirable results because of how the system was designed, not because of defective operation of any specific part

of the system. This coordination flaws are particularly evident when looking at information flows and the operational disruption that could happen due to cyber-attacks to these information flows.

The underlying basic assumption for any systemic approach to risk management is that the optimization of individual components or subsystems in a system does not in general lead to the optimum of the system. Rather, the optimization of one part of the system may actually worsen the overall system performance (Leveson, 2005, p.141).

A systemic approach to risk management is not something new. Jay Forrester, starting from the application of control theory to organizations, proposed an approach for understanding the structures that make systems behave the way they do. In the seminal work “Industrial Dynamics” Forrester analysed in detail the influence of structure on the performance of supply chains, and developed both a graphical and a mathematical language through which to represent these structures and to derive management implications (Forrester, 1961). Figure 29 shows a representation by Forrester (1961) of what he called a “*production-distribution system*”

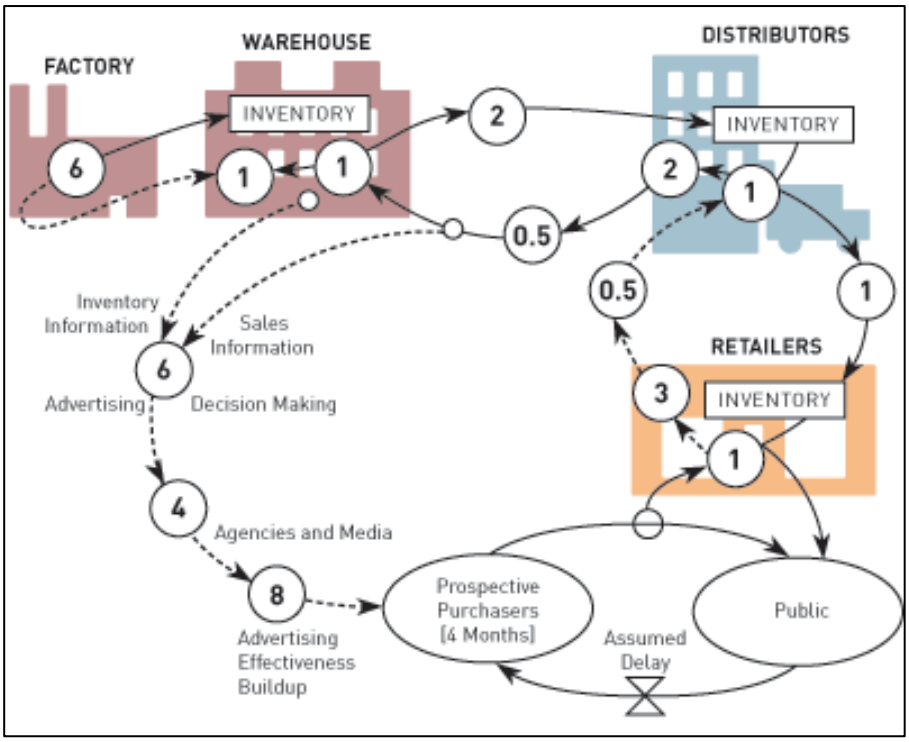

Figure 29 Production-distribution system (Forrester, 1961)

Special attention was given to the value of information, particularly concerning that "*information sources, like other flows in the industrial system, are subject to being distorted*" (Forrester, 1961, p.427). The implications and advantages of using a dynamic analysis to understand information resilience cannot be overstated. As an example of the power of this approach, Forrester's application of a time-dependent, i.e., dynamic, analysis resulted in relevant insights:

- The bullwhip effect was uncovered. Also known as the Forrester effect, it is "*the progression toward the factory of the disturbance that is created by the change in retail sales*"

experienced as a "*progressive increase in the peak ordering rate as the disturbance moves upward in the system*" (Forrester, 1961, p.173). Based on the system shown in Figure 29, Forrester goes on to show how a step increase in retail orders results in behaviours to the distributor, wholesaler and factory of increasing distortion, as can be seen in Figure 30, where the manufacturing orders to factory have much larger swings (bigger amplitude) than the orders to distributors from retailers for example. This insight is not merely theoretical but has been experienced by anyone who has had the change of playing the "distribution game" (Sterman, 1989). This management game was derived from Forrester's work and consists of a simplified version of a supply chain that has to be managed to cope with variations in demand. Despite the apparent simplicity of the game setting, participants routinely experience uncontrolled variations in inventory throughout the game, without any external influence, just due to the structure of the supply chain before them and their decisions.

- Availability of information can be harmful. From Forrester's analysis in the "*Industrial Dynamics*" book, and while arguing for the real value of information, proposing that "*the result of more timely information can be harmful. The effect can be to cause the manager to put more and*

more stress on short-range decisions" (Forrester, 1961, p.427).

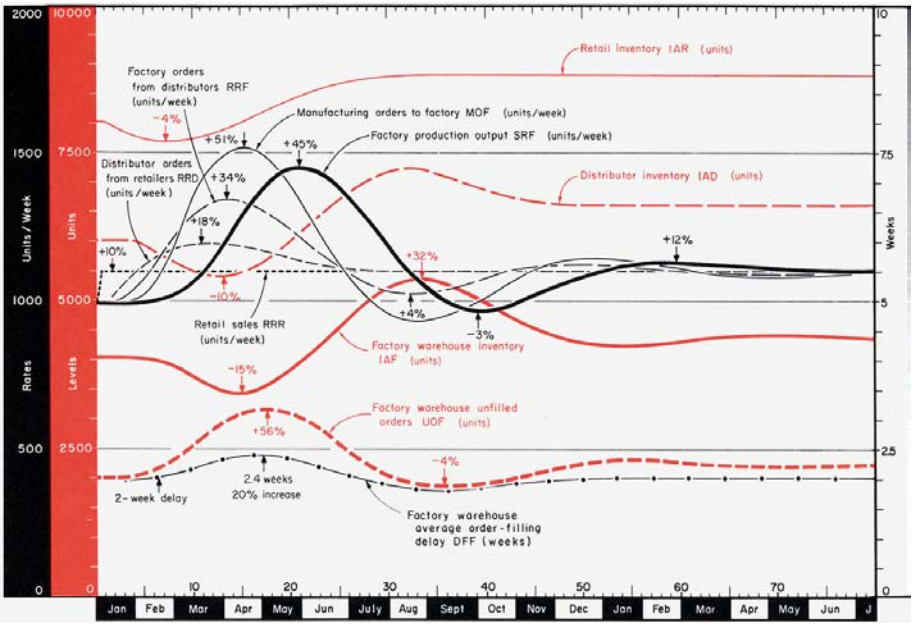

Figure 30 System response (Forrester, 1961)

- More recently, Sterman et al., (2015) have further extended the unexpected consequences of a dynamic supply chain creating unwanted behaviours despite all components working as expected, through what they have called "*phantom ordering*" or the effect through which the orders in the supply chain are inflated as a result of bounded rationality and emotional reactions to a perceived future scarcity, introducing the human factor as a central aspect in modelling risk for supply chains.

Forrester did not mention risk in his work (Forrester, 1961), but considered system disruption by using exogenous variables (p.112) through which external shocks to the model were introduced to test its reaction. More recently, the use of switches to explore different internal information flow disruptions has also been proposed (Rahmandad et al., 2015). As such, despite risks not directly being addressed, their effects are nevertheless simulated and analysed.

The existence of risk beyond component failure was identified by Charles Perrow (1984). These risks were denominated "*system accidents*" and are caused by the complexity of interactions and the presence of tight coupling, i.e., a system where software and hardware are not only linked but also dependent on each other. Perrow does not mention circular causality directly, but the definition of system accident requires mutual interaction.

Others have addressed specifically the analysis of risk through systems thinking approach. White (1995) suggested the use of a systemic approach to understanding and managing risk as a result of studying existing risk assessment methods, suggestion driven by both the increasing number of hazards and failures that accompany the adoption of new technologies, and the different shortcomings in existing methods to manage this complexity.

Carroll (1998), for the case of industries with high levels of hazard, highlighted that "*a high level of complexity and the tight*

coupling among problems seems to require a more comprehensive [approach] than those typically employed" suggesting that traditional solutions, although well-intentioned, fail to help through their unintended side-effects. Carroll goes on to indicate that well-intentioned commonplace solutions can actually hinder improvement, and even exacerbate the problem these intended to mitigate. He, therefore, proposes a problem-solving dynamic that would include both problem fixing and goal learning, as well as "*modelling tools to organize dynamic interdependencies, and feedback about effectiveness*" (Carroll, 1998). Figure 31 is a representation by Carroll that illustrates how two possible fixes, in this case writing detailed procedures and disciplining workers, can have unforeseen side-effects that make the original problem worse, in two vicious circles, known in the system dynamics community as reinforcing feedback loops (for more information about feedback loops, see the System Dynamics section of this thesis).

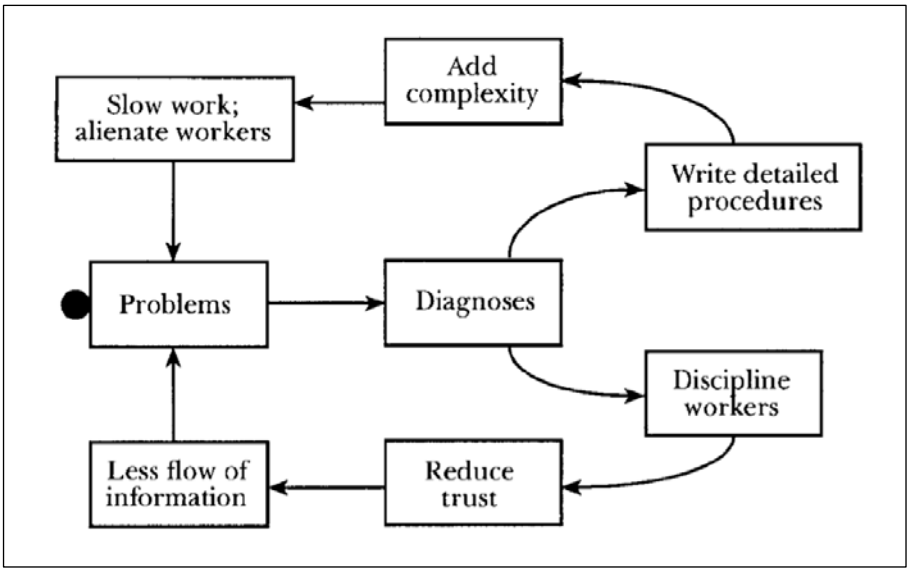

Figure 31 Representation of fixes that fail (Carroll, 1998)

What is characteristic in Carroll's approach, is the proposal of risk as generated internally by the organization, as in the case shown in Figure 31, there is no outside intervention in the loops that maintain the problem going, but rather it is created by the organization's own structure.

Kang and his team have used a systems approach to identify what they called Limiting Conditions for Operation (LCOs), a concept that is extensible to supply chains (Kang et al., 2005). Their paper mentions three important aspects: 1) a systemic approach ensures a causal relationship in the establishment of the feedback loop structure, 2) the approach is useful for understanding the behaviour of a complex system over time, and 3) a systemic approach is useful in conceptualizing a thorough

understanding of human interactions within complex systems. Although Kang uses a systems approach for modelling, the feedback loops structures are not mentioned, and several of the relationships are expressed in probabilistic terms. It does however maintain the focus towards structures in the system that generate and maintain the behaviour that is seen.

A method for analysing risk based on systems theory was proposed by Nancy Leveson and her team in 2011, based on several shortcomings seen for existing risk analysis methods to respond to the requirements of the market, such as the exponential creation of new paths to systems failing due to technological innovation, a reduced ability to learn from experience due to the fast pace of technological change, the changing nature of the ways in which the systems can fail due to the technological innovation, new types of hazards, an increasing complexity and coupling of systems, a decreasing tolerance for single accidents, a difficulty in selecting priorities and making trade-offs, an increasingly complex interaction between humans and technology, and changing regulatory views about safety, for example (Leveson, 2011). The proposed method is named STPA (Systems Theoretic Process Analysis) and belongs to the family of failure tree analyses, yet differs from them by adopting a meta-causal approach. Instead of looking at the individual actions that lead to the operational disruption, STPA considers the systemic situations (called hazards) that lead to these disruptions, to then identify the

conditions in which actions already designed into the system (called control actions) can lead to these hazards and thus to the situations that want to be avoided (called losses).

More recently, Ghadge et al. (2013) proposed a systemic approach based on three pillars of risk analysis: risk identification, risk assessment and risk mitigation. Their proposal considers the generation of a system dynamics model containing different attributes and parameters, where risks can be simulated over time (dynamically) and sensitivity analyses can be obtained about the relevance of each parameter. Despite the results and simulation clearly pointing out to a system dynamics model, it is unclear what feedback loops, delays and sources of inertia, i.e., stocks (Sterman, 2000) were considered. Ghadge et al. (2013) concentrate on the identification of impacts and the occurrence of other impacts within the organization as a result, this causality being represented by probabilities. Two shortcomings can be mentioned for this approach. First, the identification of impacts and their probabilistic relationship to other impacts requires historical information that, for events that are uncommon or that have not been experience before, is not available. Second, even if the probabilistic relationships between impacts is known, this sole relationship is not actionable in any way, as this relationship does not deliver any information on the mechanisms that originate this causality, and therefore neither result in recommendations for prevention nor mitigation. As a result, despite being focused

towards the risk that is created by the organization's own impact-contagion or transference, the approach by Ghadge et al. (2013) does not lead to practical implications for companies.

Garbolino et al. (2016) and his team have used system dynamics modelling and risk analysis to propose a dynamic risk analysis method that includes both constraints and behaviour over time (dynamics). Their modelling approach focuses on the strengthening of constraints, and models organizations as managing a dynamic process where industrial systems continually adapt to external and internal changes to achieve their goals. The model proposes a ten-step approach that culminates in structured scenario analysis, where the system is tested against different boundary conditions of interest. It is however restricted to a single plant and its internal process, thereby lacking the integration with other supply chain partners.

The comparison of the methods just mentioned is shown in the next table, where these are compared with the criteria that need to be considered for answering the research question.

Table 20 Comparison of systemic risk analysis method

	RSQ4.1.- How can a systmic risk analysis apporach mitigate compartmentalization, static framework and historical dependence for managing cyber risks in the supply chain?					
Framework	**Risk Analysis**	**Systems thinking**	**Integrated**	**Dynamic**	**Non-historic**	**Yes/Total**
Forrester, 1961	No	Yes	Yes	Yes	Yes	4/5
Carroll, 1998	Yes	Yes	Yes	No	No	3/5
Kang et al., 2005	Yes	Yes	No	Yes	No	3/5
Leveson, 2011	Yes	Yes	Yes	Yes	Yes	5/5
Ghadge et al., 2013	Yes	Yes	Yes	Yes	No	4/5
Garbolino et al., 2016	Yes	Yes	No	Yes	No	3/5

From this table it can be seen that Leveson (2011) fulfils the most of the criteria associated with research sub-question 4.1, addressing all five of the points associated with the question. It addresses integration, it is a dynamic approach, does not rely on historical information, is focused on analysing risk, and considers a systems thinking approach. The next section describes the process, and the data gathering and analysis it involves.

3.8.2 Systemic risk analysis through STPA

The Systems Theoretic Process Analysis (STPA) method is based on the fault tree analysis family of methodologies. The fault-tree family is all those methods that start from an unwanted result and seek back for the causality that originated this result.

Fault tree analysis (FTA) was developed in 1961 by H.A. Watson at Bell telephone laboratories and is a method mainly used for the identifying what causes a hazard, not for identifying the hazards themselves. FTA uses Boolean logic to identify and

describe the combination of faults that lead to an unwanted hazard, and is thus a top down method, starting from the hazard and drilling down through causes for that unwanted condition up to the basic or primary events, as can be seen in Figure 32. The FTA process has four basic steps: 1) system definition, 2) fault tree construction, 3) qualitative analysis, and 4) quantitative analysis. The FTA process provides no indication on how to define the system or the top events, and the basic or primary events could either require probabilistic information or are related to structural properties of the system.

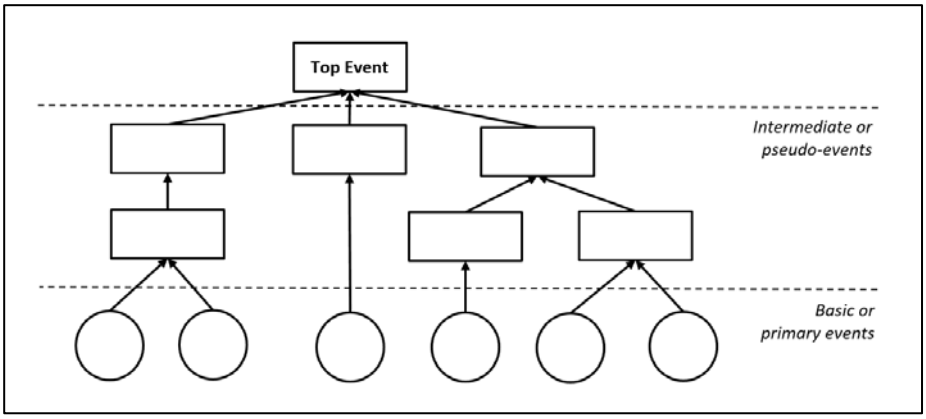

Figure 32 Fault tree representation

STPA, starting from the general principles of FTA, goes on to adopt a meta-causal approach: instead of looking at individual actions that lead to undesirable outcomes, STPA considers the systemic situations that lead to these losses- called hazards- to then identify the conditions in which the actions already designed

into the system - known as control actions - can lead to these hazards and thus to the losses that want to be avoided.

STPA assumes an internal source of risks - endogenous view of causality - by understanding failure as a result of the structure of the system, and not due to external factors of the disruption, being thus a method based on systems theory rather than traditional analytic reduction and reliability theory. According to the systemic view, design constraints for the system (or the lack of these) are the causes of an undesired outcome. It is thus a complementary approach to protection from external threats, by focusing on protecting the system "from its own design". A safe operation (free of unwanted events) is seen as an emergent property resulting from the interactions between the system components and with the environment. The problem of avoiding "accidents" (i.e., unplanned loss events) thus becomes a dynamic control problem of limiting the ways in which the system can behave by designing the structure underlying this behaviour.

From this perspective, cyber-attacks are not merely events that happen to supply chains, but rather events which supply chains are "misdesigned" to experience. Cyber-attacks are thus unintended consequences (Sterman, 2001) that result from incomplete requirements (Leveson, 2011) at the time of supply chain design, and that are originated in a structure that allows these attacks to occur. A systemic analysis seeks to identify this "unrequested"

design that results in cyber-vulnerability, and determine structural changes through which a cyber-vulnerable behaviour is less likely to occur or no longer possible.

The use of systems thinking for the understanding the requirements for a safe system operation is based on some general principles for systems safety (Leveson, 2005):

- Emphasis on safety *during system design* and construction, not in adding to a finalized design. In this case it joins the traditions followed by disciplines such as maintainability (Smith, 2017) and constructability (Tatum, 1987) that require aspects for effective maintenance and construction to be added at the system design stage, respectively,
- Consideration of *the whole system* rather than components or subsystems,
- View of *hazards beyond only component failures*, aspect which differs from the computer safety approach,
- Emphasis of *analysis rather than standards or past experience*, aspect which requires understanding the structures that cause an accidents before these occur,
- Emphasis on *qualitative rather than quantitative* approaches, as the quantitative data at the time of design is limited on inexistent,
- Recognition of the existence of system trade-offs and conflicts in systems design, since "*no system is absolutely*

safe, and safety is not the only and rarely the primary goal for building systems" (Leveson, 2011).

Literature has been published about the STPA methodology framework (Estefan, 2007; Leveson, 2011; Salmon et al., 2012; Altabbakh et al., 2013), with examples of its application in several domains, such as medical industry (Antoine,2013), environmental studies (Hardy et al., 2011), robotics (Mitka et al., 2015), power production (Karami et al., 2015), software development (Wang et al., 2016), aerospace (Ishimatsu et al., 2014) and defence (Chiesi, 2016), to name a few. No application has been documented however for supply chains or cyber-risks in supply chains. The research process did not find documented literature on the application of systemic risk analysis methods such as STPA in supply chains or to cyber-risks.

Additionally, the STPA methodology is advanced through an annual spring workshop (March-April) held at the Massachusetts Institute of Technology in Cambridge, MA, USA. Under the leadership of professor Nancy Leveson PhD., and John Thomas, PhD., where the application of STPA and other derived methods are shared[5].

[5] The latest workshop was held in 2017. For more information : https://psas.scripts.mit.edu/home/2017-stamp-workshop-registration/

The process of STPA is based on the STAMP principles, the Systems Theoretic Accidents Model and Processes, a conceptual framework based itself on systems thinking, and which understands causality of unwanted events or "accidents" as derived from the disrupted system itself rather than externally. As such, STAMP it is the theoretical foundation for different tools for more specific applications (Leveson, 2011), as shown in Figure 33. STPA deals with an analysis before an accident has materialized, and is therefore an ex-ante analysis, based on the STAMP framework. Another technique that is available derived from the STAMP framework but which is not used in this thesis, is CAST, or the Casual Analysis based on STAMP, for the analysis of scenarios where an accident has already occurred, being therefore an ex-post analysis.

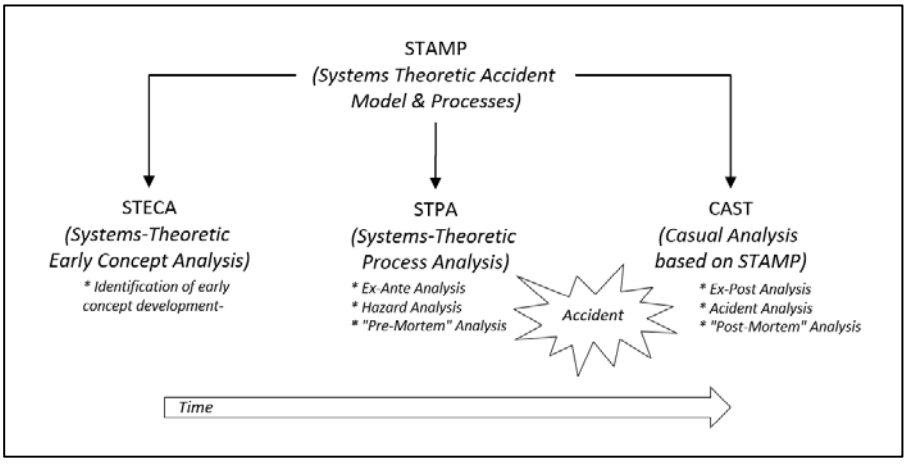

Figure 33 STAMP framework and derived techniques

In systems theory, and thus in the STAMP framework, emergent properties such as safety or resilience originate from the interactions between the components of the system, and are controlled by imposing restrictions on that level from a higher level of hierarchy. Emergent property behaviours therefore becomes a control problem, where the goal of the control is enforcing these required constraints during design and operation of the system. According to STAMP, preventing unwanted events from occurring requires a paradigm shift from avoiding failures from a process, to a broader goal of "*designing and implementing controls that will enforce the necessary constraints on the process*" (Leveson, 2011).

STAMP is thus based on three overarching concepts:

- *Safety Constraints*, a basic element in STAMP as accidents occur when the required constraints have either not been designed into the system, or, have not been enforced.
- *Hierarchical Control Structure (HCS)*, levels of aggregation where emergent properties of interest manifest and can be managed. Hierarchy is used to describe accidents in terms of adaptive feedback mechanisms (see Figure 34) through control actions on a controlled process that respond to feedback signals from that controlled process. The controller is in a different level of hierarchy and the control

actions are conditioning the ways in which the controlled process can behave.

- *Process Models*, which are the abstraction about the controlled process and about the controller actions that the controller has available, and based on which the decisions are taken. As seen in Figure 34, the process model is distinct from the controller, but a crucial part of it, as it is through the process model at the controller that the control action decisions are taken during adaptive feedback.

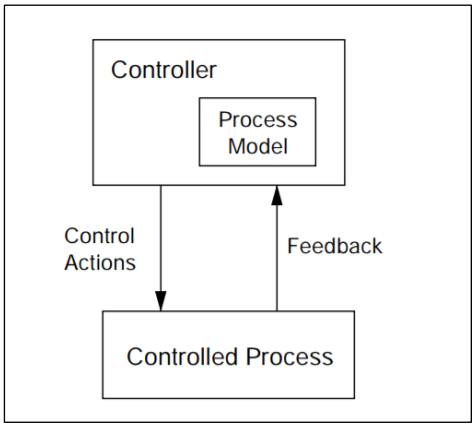

Figure 34 Adaptive feedback mechanism (Leveson, 2011)

The process model contained in an organization includes all algorithms that are used by automated systems, as well as the mental models that agents in the organization have about how the organization works, or those ideas members of the organization have to explain how business and the outside world operate (Morecroft, 1992). For example "*if you understand inflation, a mathematical proof, the way a computer works, DNA, or a*

divorce, then you have a mental representation that serves as a model of an entity in much the same way as , say, a clock functions as a model of the earth's rotation" (Johnson-Laird, 1983).

3.8.3 Data gathering process and data analysis

The data for this research was primary data collected from interviews. A total of 18 interviews were carried out to workers in 3 plants of the company. These workers were members of the Supply Chain Management, Finance, warehousing Production, Quality, and from a main supplier. A research protocol was created and followed in all interviews, and it has been included in section 11.10 of the Appendix.

The process of systemic risk analysis based on STPA considers the following steps (Leveson 2011):

- Identify the system that is considered for analysis. Consistent with the systems thinking framework, this system is defined by the system goal, the controllers that are part of the system, the information flows present in the system, any storage of information present in the system and the control loops that are present in the system. The Controllers are any agents in the system that have the ability of sending or receiving information, such as an operator, or an automated system for decision making.

- Identify the control actions that can be effected by the controllers identified for the system. These control actions are any processes carried out by the controllers to influence the system.
- Identify the unacceptable losses in the system. Considering the goal of the system defined earlier, the unacceptable losses are those events that jeopardize the goal, including the loss of human life or human injury, property damage or environmental pollution.
- Identify the hazards present in the system, i.e., the system states or a set of conditions that together with a worst case of environmental conditions lead to an unacceptable accident.
- Identify the unacceptable control actions. Considering the unacceptable losses, hazards and control actions of the system, determine when a control action leads to a hazard. For the case of cyber-risk context, the environmental conditions are those derived from a cyber-attack.
- Identify those unsafe control actions that are enabled by cyber attacks
- Identify security requirements or system design requirements to avoid the unsafe control action. These requirements and design considerations allow for modifications to the existing system.

This whole process can thus be considered as a balancing loop aimed at minimizing the number of unsafe control actions in each iteration. This process is shown in Figure 35.

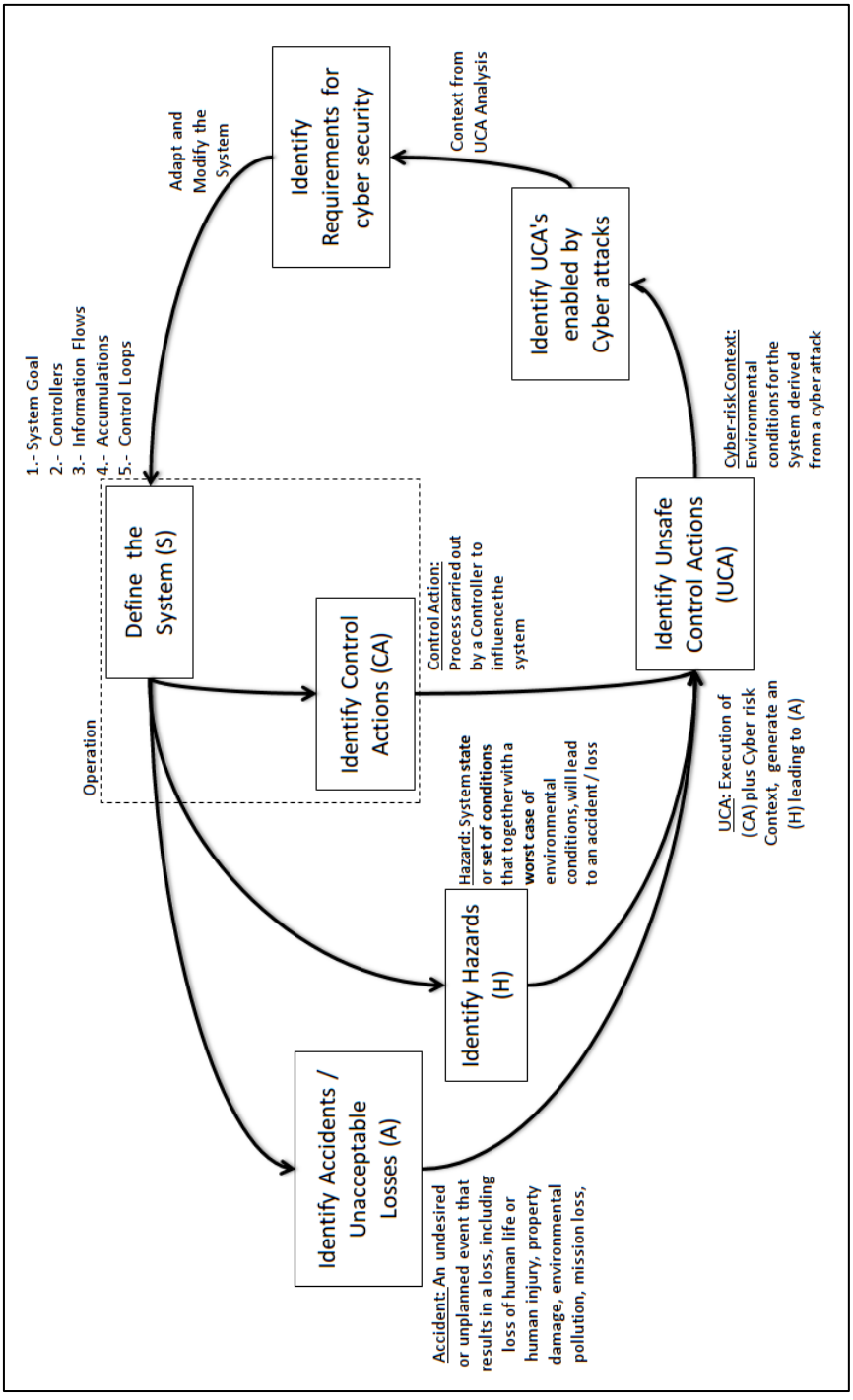

Figure 35 STPA process applied to cyber-risks

The process as laid out conditions both the type of data that is gathered and the way in which this data is gathered, since information has to be collected from the case company and organized according to the requirements and structure of the method. The method that is used is a case study method with a directed analysis.

Case study research is especially well suited and is "*the preferred strategy when 'how' and 'why' questions are being posed, when the investigator has little control over events, and when the focus is on a contemporary phenomenon within some real-life context*" (Yin, 1994). This constitutes a fit with the characteristics of the problem this research project is trying to model: cyber-risks to the supply chains is a phenomenon that is currently evolving (contemporary) and the effects are not under the control of the investigator.

As shown by Ellram (1996), a case study strategy is the chosen type for empirical data that is mostly qualitative, as seen in Figure 36.

Type of Data	Types of analysis: Primarily Quantitative	Primarily Qualitative
Empirical	Survey Data, secondary data, in conjunction with statistical analysis, such as: factor Analysis cluster analysis discriminant analysis	Case studies, participant observation, ethnography. Characyerized by: limited statistical analysis, often non-parametric
Modeling	Simulation linear programming mathematical programming decision analysis	Simulation role playing

Figure 36 Research design (Ellram, 1996)

It has been argued that despite being intellectually demanding, the use of systems thinking for analysis of failures "*offers the best chance of identifying contributory factors*" (Bennet, 2016).

3.8.4 Software used

The process of defining the system, unacceptable accidents, hazards, controllers, control actions unsafe control actions and derived requirements is a process that results in a complex network of relationships. These relationships can and have been managed through either relational databases or related spreadsheets. However, software has been developed that makes this process not only manageable, but allows for a structured approach.

This thesis is using a mixture of spreadsheets and specialized software to manage and analyse the information that is obtained through the STPA modelling process.

The Software that is used is called XSTAMPP[6], a platform developed at the University of Stuttgart in Germany, to serve as a support tool for the STPA hazard analysis process (Abdulkhaleq et al., 2015). The information that was gathered in the XSTAMPP tool is stored in XML format. After having gathered the information in XSTAMPP (See Figure 37), this is then "*translated*" into Microsoft Excel sheets through a small python routine (See Appendix 0) to transform the XML data into text data. Excel is then used to derive the frequencies and probabilities.

[6] http://www.xstampp.de/

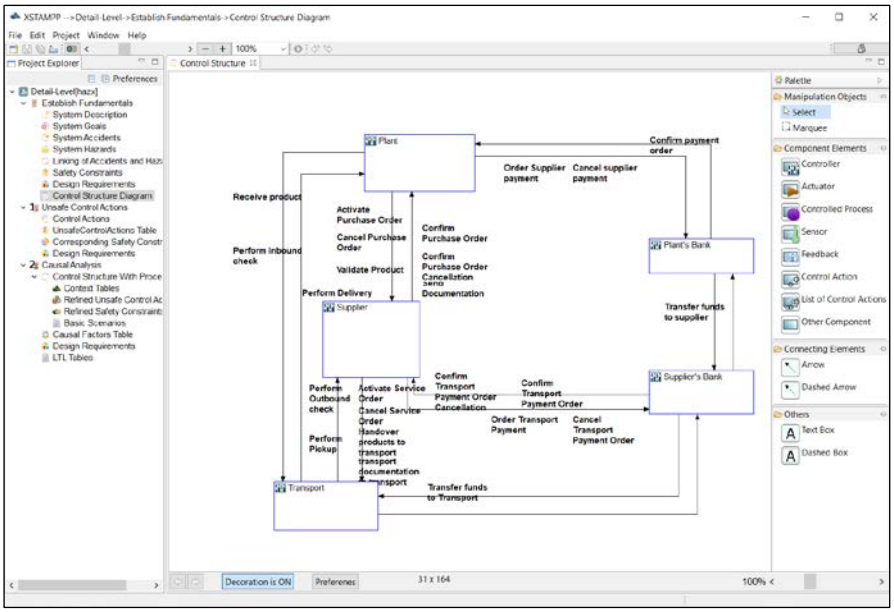

Figure 37 XSTAMPP analysis tool for STPA process

3.8.5 Case selection

The STPA analysis requires information about organizations that are exposed to cyber-risks and, more importantly, that perceive the need to prepare for these risks. Yin (1994) indicates that in contrast to strategies such as surveys which rely on sampling of a representative population, the number of cases to be used in a case study is determined by "*saturation*" i.e., the number of cases required when no new findings are revealed through the data from additional cases. The saturation is therefore reached through a sequential discovery, as it is not possible to know the number of cases required if these cases are developed in parallel by a group of researchers until these are compared. In the case that the process in being executed by a single researcher, the only way

to find saturation is when the last case that was obtained did not, in fact, add new information from the one that was already obtained from previous cases.

Additionally, due to time constraints, the number of cases can also impact the depth to which each individual case is researched (Sanders et al., 2016). The larger the number of cases, the less individual information that can be obtained.

It is finally Yin (1994) that provides the strongest argument toward the number of cases required. The research question RSQ 4.1 wants to explain the way in which a method already successfully applied to other domains, can be useful for the case of cyber-risks in supply chains. This context is indicated by Yin as the rationale for selecting a single case for representing the critical test of a significant theory. Additionally since STPA has not been used for the analysis of cyber-risks in a supply chain before, thus corresponding to a revelatory case, where the information and its analysis uncover new information.

3.9 Research design – Dynamic modelling

This section presents a justification for the choice of a dynamic simulation through system dynamics for understanding cyber-resilience in supply chains, the data gathering process is laid out, and the case selection is described.

3.9.1 Why modelling

Complex systems defy intuitive understanding, as is revealed in the statements that justify this thesis research: despite existing risk management processes, and the great investments that are carried out to advance cyber-security, cyber-attacks continue to occur with disruptive consequences for supply chains. From a systems thinking perspective, this "*counterintuitive behavior*" has many potential origins of which Sterman (2000) highlights: limited information, confounding variables, ambiguity, bounded rationality, misperceptions of feedback, and flawed cognitive maps, all of which lead to erroneous inferences about the management of the dynamics of the systems. This error is compounded by human biases of which many are invisible in daily decision making, defensive routines to justify flawed mental maps and biased decision-making, and the imperfect implementation of those decisions.

In order to manage this troubled access to reality, "*virtual worlds*" (Schon et al., 1986) have been proposed, through formal models that create virtual simplified versions of reality, or "*micro worlds*" (Papert, 1980), that are simulated as "*reliable substitute descriptions that can help one understand a real system and its expected behavior*" (Bossel, 1994, p.4). These virtual worlds are sometimes the only way of analysing situations such as

emergencies in advance of them actually happening, potentially providing high quality outcome feedback.

The use of models to understand socio-technical systems comes from a western tradition where "*whatever happens is not believed to be random; it is assumed to have a cause that can be understood and probably altered*". Additionally "*modelers have a managerial world view [according to which] problems should be actively solved, not passively endured*" (Meadows, 1980).

The importance of the modelling of organizations was well described by Jay Forrester in the 1960's already. He indicated that when people were asked "*who is the most important people in the safe operation of an aircraft?*" most would answer that those were the pilots. However, despite the extreme relevance of skilled and well trained pilots in the operation of an aircraft, what is rather more important is the design of an aircraft that can have a stable and robust operation in extreme conditions, and which ordinary pilots can fly even if they are tired, stressed of flying in unexpected conditions (Sterman, 2000). Forrester indicated that too many manager spend time performing as pilots, through activities such as decision-making and taking control from subordinates, rather than designing and implementing an organizational structure that can be managed well by ordinary people (Forrester, 1965). Therefore the role of the executive level should be one of corporate design and not corporate operation.

Management engineering research, or the research for effective engineering of the management activity, is a materialization of this vision, through the generation of models, as "*CEO's will eventually have to be competent in the creation and use of models if they are to lead such [organizational] planning activity effectively*" (Keough et al., 1992).

Simulation is an essential part of training for the military operatives, pilots, power plant operators and medical doctors, examples of activities where human operators interact in real time with complex technical systems. However, the use of simulations in management is less common despite also having a long history, as a minimum going back to the "*Beer Distribution Game*" (Sterman, 1989), a board game developed by Jay Forrester to model a simple supply chain (Forrester, 1961). These applied simulations have been named "*management flight simulators (MFS)*" (Sterman, 2014) or "*policy flight simulators*" (Rouse, 2014), and provide "*low cost laboratories […] that allow time to be compressed or dilated [and where] actions can be repeated under the same or different conditions*" (Sterman, 2000, p.35). The learning process that happens through the use of these virtual worlds is illustrated in Figure 38.

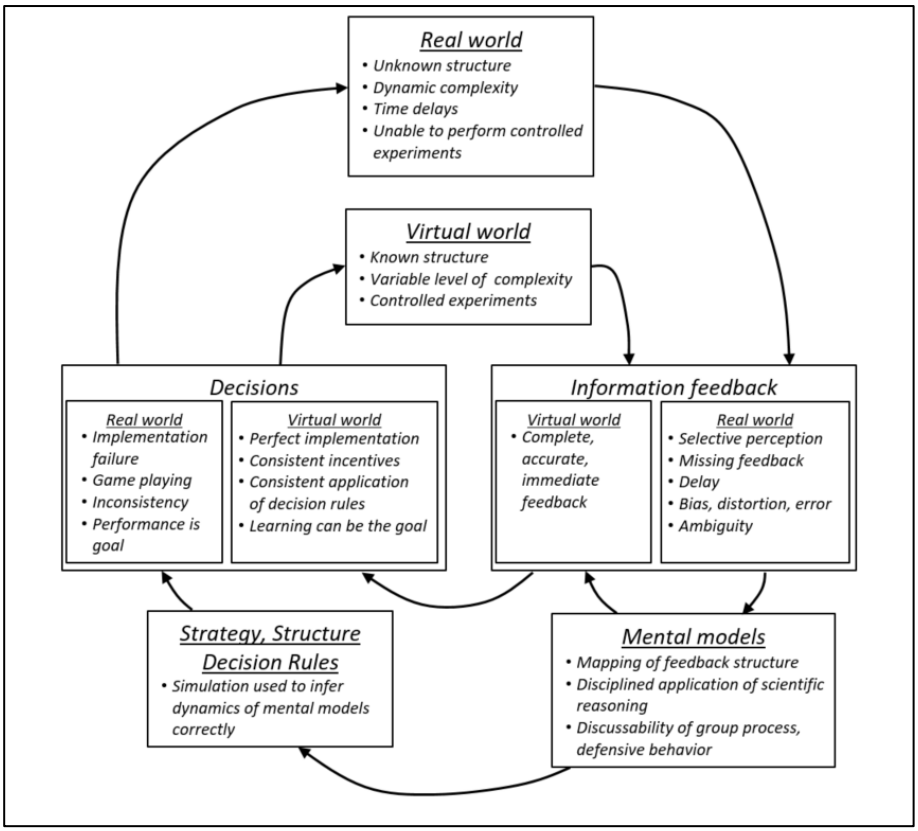

Figure 38 Process with virtual and real worlds (Sterman, 2000)

The process that is followed is understanding the real world through the use of a virtual world environment to make up for the difficulty of accessing the real dynamic complexity and unknown structure of the real world that needs to be managed,

Models and simulation are an innate part of or human experience. As Bossel (1994, p.1) describes:

"As we get up in the morning, we crank up our mental model of the little world around us, run a few simulations in our mind on how we are going to deal with the problems and people we meet

during the day, try out different approaches, evaluate the likely outcomes, and start the day with a plan. It will not protect us from failures and surprises, but it will have prepared us to deal more effectively with whatever tasks await us"

Through modelling, existing knowledge about a system and the way in which these characteristics interact to condition the behaviour of that system, are used for design and management purposes. Modelling assists the unreliable ability to understand interactions in systems beyond only the individual parts, by allowing the visualization of these interactions and their effects. As Morecroft (2015) describes it, the goal of a systemic simulation is "*the redesigning of social and business systems so that, despite their complexity, normal people can run them competently*" (Morecroft, 2015, p.21).

Some desirable characteristic of models include: its capacity to generate insights or new ideas, some degree of descriptive realism, their capacity to reproduce modes of behaviour from the real world, its degree of transparency and capacity of being understood by a non-specialist audience, the relevance of the problem being addressed by the model, its capacity to incorporate additional findings to modify structure and test outcomes, and its capacity to replicate real-world observations and to predict behaviour (Randers, 1980).

The use of modelling to drive policy facilitates the exploration of a problem space with an inductive instead of a deductive approach. When understanding a problem deductively, data gathered in the field is used to prove or disprove a theory represented as hypotheses about the world. Instead, with an inductive approach, the problem space is an open field of possibilities, the data gathering can be a little fuzzier, yet allowing the discovery of patterns or relationships that were previously unknown.

Everyone has their models of the world. More than a choice, modelling has been argued as a way in which to have some "*knowledge of the future*" to identify the potential actions. A person knows when to cross the street, a student selects a major for the next four years, a general decides to position its dissuasive forces, or a buyer decides to raise a potential flaw in its computer systems, all according to the mental models they have about the world in which they operate.

Mental models, having been built from past experience, accumulate observations and resulting generalizations of what happened in the past. However, the past is not well known either. Research has shown repeated evidence of the unreliability of human memory, full of conceptual and perceptual biases, many of them unrecognized and subconscious.

In the case of increasingly complex social systems, the interaction between members of these systems drives them to perpetually compare their mental models as a result of individual or joint decisions on their common organization. However, mental models are not directly transferrable from one mind to another, and it is not an intuitive task to translate mental models into the symbols and language necessary to convey them to another, as these mental models are usually non-sequential, unstructured and diffuse. Despite these apparent "shortcomings", mental models seem to allow people to function reasonably well in a changing and variable environment.

3.9.2 Why System Dynamics

Frederick Taylor is regarded as one of the earliest proponents a scientific approach to solving management problems, and the early identification and application of scientific principles was based on the study of problems in a factory shop floor, in what can be regarded as the birth of Operations Management. Through the application of analytic techniques to operational processes, an efficient utilization of resources was sought by identifying the activities that were needed, identifying those activities that were not needed, sequencing the activities, and arranging them spatially to maximize the use of existing resources (Taylor, 1914). As such these earlier versions of scientific management were rather engineering activities rather than the development of science, as it

lacked an underlying generic knowledge about the processes it was managing.

However, despite this lack of underlying science, scientific management has been be extremely successful (Waring, 2016), and at its early stages it facilitated the rise of consultant companies between the first and second world wars (Kiechel, 2010), and of industrial engineering schools seeking to teach these methods through simplified problems, also called "*idealized problems*" (Will et al., 2002).

Idealized problems are stated in simplified and partial terms by presenting only those aspects required to the use of the method being taught, and with no reference to any particular industrial instance of the problem. Examples of this include inventory control problem, scheduling problems, routing problems, maintenance problems or any type of statistical control. The increase in the complexity of the problems to make use of the progress in computing power, and mathematical and statistical techniques, gradually gave rise to the Operations Research discipline, as a branch of computer science and applied mathematics, and it has been described as "*quantitative research within Operations Management*" (Will et al. 2002).

It has been argued that the development of Operations Management, both in qualitative and quantitative initially lacked in the delivery of scientific models of operational processes with

predictive power, rather producing techniques that were partially useful, but that did not have explanatory power. First, the identification of patterns based on the statistical analysis of historical data allowed the development of strong short-term forecasting techniques. However, these techniques did not develop any causal relationships to explain or predict behaviours, acting rather as a black box. Second, the development of Inventory control methods allowed for the optimal of good approximate solution of that type of problem, again without any underlying structure that allowed for explanation of prediction of behaviour. As such, these were static analyses.

Two important exceptions that challenged this static approach. First, queuing theory was proposed as a way of modelling the stationary behaviour of a system when considering variability in the orders arriving to the production system, and available resources, providing a framework with a flexibility that allowed for the use of probabilistic uncertainty, and stochastic processes, for example. Second, the development of system dynamics in the 1960's provided a framework for understanding the non-stationary behaviour of a system as derived from the feedback structure of the system. For a detailed discussion about system dynamics, see section 3.2.3.

Will et al. (2002) classifies therefore Operations Management model-based research into two recognizable classes: axiomatic and empirical.

The *axiomatic model-based research* is driven mainly by the idealized model itself. The objective is to derive insights of the model as defined for the problem, deriving information about certain variables in the model from assumptions in other variables in the same model. There is a use of formal methods developed by statistics, mathematics or computer science, and researchers in this line have training in areas such as queuing theory, Markov processes, decision theory, dynamic programming or mathematical optimization. It is thus a deductive research approach considering a system in a stationary condition[7].

On the other hand, the empirical model-based research is an Operations Management research class with strong emphasis on the coherence between what can be observed from reality and the model made to approximate that reality. This class has therefore a close alignment with the virtual-worlds approach discussed in section 3.9.1. It is an approach that is mainly inductive, used for

[7] A stationary condition of a system is a behaviour (value over time of the states of the system) that has a probability distribution function that does not change over time.

the analysis of systems in a non-stationary condition. Research done in this line includes the industrial dynamics stream developed by Forrester (1961) which later evolved to business dynamics (Sterman, 2000), and research about the clockspeed in industrial systems by Fine (1998), and Mendelson et al. (1998).

Both classes partly derive their validity from the degree to which their model solutions assist managers in making decisions in the real world (Will et al., 2002). These two classes are compared in Table 21.

Table 21 Axiomatic vs. empirical model-based research

Aspect	Axiomatic	Empirical
Approach	Mainly Normative, some descriptive	Mainly descriptive, some normative
Inference	Mainly deductive	Mainly inductive
Focus	Model	Model correspondence to reality
Academic methodology discussion	Weak	Strong
Task analysis	Stationary behavior	Non-stationary behavior
Scientific relevance	1.- New variant of existing problems 2.- New solution techniques to existing problems 3.- Improved solutions to existing techniques and problems	1.- Model recognized as an aspect model of reality 2.- Tests and challenges the validity and usability of theoretical models
Model presentation	Formal mathematical terms	Representation of a structure that leads to process behavior
Researcher background	Mathematical analysis, Numerical analysis, Computer science	Conceptual modeling, Operations
Example Methods	Queuing, Regression analysis, Linear programming	System Dynamics Agent Based Modeling

Therefore, from the need to model reality for identifying and understand structures behind the behaviours of a supply chain, and according to the empirical model-based research class within Operations Management, is that system dynamics has been chosen as the method to develop the model for this part of the thesis.

3.9.3 Data gathering process and analysis

The objective of this research protocol is to describe and prescribe a reproducible data gathering and analysis process. This process results in the development of a series of representations of the dynamic (time-dependent) structure and response of a supply chain when faced with a cyber-attack. These representations are causal loop diagrams, a hierarchical control structure and a system dynamics model.

The purpose of the study is threefold: 1) to gain some insight into the supply chain structures that partake during a cyber-attack, 2) to understand the relationship of this structure the organizational reaction and performance to the cyber-attack, and 3) to identify and test the main factors that influence that reaction and performance.

As a source of information, this study uses information from four semi-structured interviews (primary data) and the gathering of documentation (secondary data). This information is about both the structure of the supply chain and the cyber-attack incident that required a response. The characteristics of the structure include information flows, information storage, regulating loops, delays, and the potential perturbations to the system. Information about the incident includes a description of the events and performance indicators during the event.

This study seeks to contribute to the scientific development of a framework for understanding resilient behaviour. The approach of using system dynamics starts from the premise that organizational structure is the source of its visible behaviour. By understanding the structure of the system it is possible to experiment with different operating conditions and as a result to design a system that exhibits the required behaviour.

Therefore, the results from applying this method evidence its capacity to address compartmentalization, static versus dynamic behaviour description, and historical dependence during its application. The analysis of this capacity, for example its range or limitations, provides information to answer the underlying research question guiding this research protocol.

The chosen method is case study with directed analysis. This analysis consists in the gathering of mainly narrative information that describes a specific situation of an organization experiencing cyber-resilience. This information is then “translated” into 1) a causal loop diagrams, 2) a hierarchical control structure and finally 3) a system dynamics model.

The gathering if the information is performed through the collection of

- Documents that describe the incident, obtained from sources within the company and from a consulting company that provided guidance during the incident.

- Documents and data from the company of its performance during the incident,
- Interviews with people in the organizations that participated during the incident. This interviews were carried out following an interview protocol.

Modelling, as seen in Figure 38, is an iterative process of hypothesis formulation, testing and revision, both of formal and mental models. The general steps in this process are (Sterman, 2000):

- *Problem Articulation*, the step to define the boundary of the problem and systems, the time frame for the study, the problem defined in dynamic terms (also called the reference modes, and some of the key variables that define this dynamic problem.
- *Dynamic hypothesis formulation*, the step to formulate a dynamic hypothesis of the problem (ideas about why the problem is occurring in the first place), and to develop representations of the problem by using the initial hypothesis, key variables, reference modes and any other available data. The available tools include model boundary diagrams, subsystem diagrams or sector maps (Morecroft, 2015), hierarchical control structures, causal loop diagrams, stock and flow diagrams and policy structure diagrams.

- *Formulation of a simulation model*, the step to specify the model structure and decision rules, to estimate the parameters, behavioural relationships, and initial conditions, and to test the model for purpose and operational ranges.
- *Testing*, the step to compare the behaviour of the model with the reference mode, to test the robustness of the model under extreme conditions of operation, and to determine the sensitivity of the parameters under plausible value uncertainty.
- *Policy design and evaluation*, step to identify and test scenarios, to test new policies, decision rules or structures, to perform what if analyses, to generate sensitivity analyses of the proposed policies, and to identify the effect of interacting policies. This process is iterative, as can be seen in the following picture.

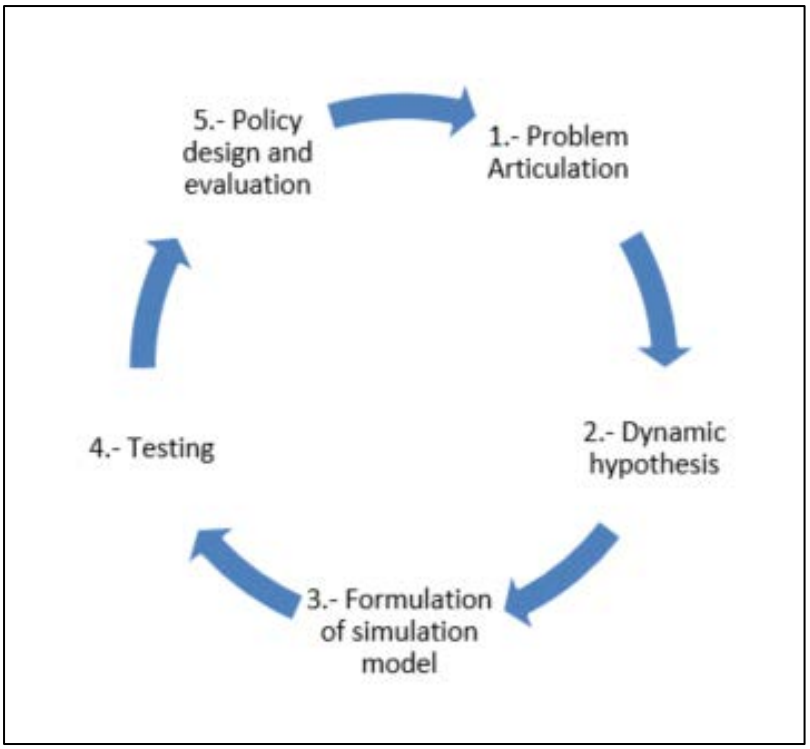

Figure 39 Modelling process (based on Sterman, 2000)

3.9.4 Software used

Two main software are used in this process: 1) a software to represent the hierarchical control structure, and 2) a software to represent the causal loop diagrams and dynamic model, and to perform the simulation.

The hierarchical control structure analysis was done through the use of a diagramming software, the "*yED graph editor*" available for download from the developer's website https://www.yworks.com/downloads#yEd.

The causal loop and dynamic model were created using "*VENSIM*" in its Personal Learning Edition PLE, available for download from the developer's website: http://vensim.com/free-download/.

These software are available for both Linux and Windows, and are freely available online.

3.10 The quality of the research design

Having outlined the research methods for answering the different research questions, is relevant to consider the elements that determine the quality of the research, this is the validity and reliability of the methods used.

The validity of the methods is the extent to which the results of the methods reflect what is intended (Sanders et al., 2016). Although "*the questions of validity can never be answered with complete certainty, researchers can develop strong support for the validity of the process*" (Dorst, 2011). Three types of validity are relevant for this research, 1) construct validity, 2) internal validity, and 3) external validity.

On the other hand, the reliability of the methods is the extent to which the method can be applied by a different researcher, delivering the same results. If a method can be applied by different researchers or at different point in time with similar results, then

the method is said to be reliable (Yin, 1994; Drost, 2011; Sanders et al., 2016).

Yin proposes a series of measures that can be used to improve the quality of each of these elements, as shown in the next table.

Table 22 Tests for research design quality

Test	Case study tactic	Phase of research in which the tactic occurs
Construct validity	Use of multiple sources of evidence	Data collection
	Establish chain of evidence	Data collection
	Have key informats review draft case study report	Writing
Internal validity	Do pattern-matching	Data analysis
	Do explanation-building	Data analysis
	Do time-series analysis	Data analysis
External validity	Use replication logic in multiple case studies	Research design
Reliability	Use case study protocol	Data collection
	Develop case study database	Data collection

3.10.1 Construct validity

Construct validity requires establishing the correct operational measures to the concepts that are being studied (Yin 1994). The validity has also been called the "*operationalization*" of the construct as it reflects the capacity of the method to "*translate a concept, idea or behavior into a functioning and operating reality*" (Drost, 2011).

Given that the collection of data is dependent on the framework that is used for analysis, the construct validity is justified differently for each of the research processes that are followed.

- For the research about the nature of cyber-risks, the data is to be analysed according to criteria of form, function, and then compared to other existing risks. Multiple sources of data were considered and there is a chain of evidence as the information can be accessed publicly.
- For the research about systemic risk analysis, the process considers multiple interviews in each case that is considered, and a transcript was created for each interview. The participants also read the report that was created after the analysis. The use of the STPA method was also justified through its successful documented application in other domains.
- For the case of the research about dynamic simulation, the process considers multiple interviews in each case that is considered. The participants also read the report that was created after the analysis. The use of the system dynamics method was also justified through its successful documented application in other domains.

3.10.2 Internal validity

The internal validity test is mainly considered for explanatory and causal studies only, where the depicted conditions and causal

relationships in fact lead to what is indicated in the research and are not the result of relationships that are not genuine (Yin, 1994).

The Internal validity is again justified differently for each of the research processes followed in this thesis.

- For the research about the nature of cyber-risks, there is pattern matching and time series analysis, to categorize the characteristics that are found, as the main purpose of the research is exploratory and descriptive.
- For the research about systemic risk analysis, since the framework used for the analysis is based on a variation of an established method, the relationships that are found are contrasted and compared between the different interviewees, to identify patterns and match their descriptions. Additionally multiple sources of data are used, including interviews and organizational documents. The explanation building from the data that is gathered, is represented in the mental maps about the organization, which are one of the results of the interviews. The internal consistency of these mental maps is a data in itself, to then compare with other performance issues.
- For the case of the research about dynamic simulation, this process is also based on an established process that has been successfully used in other domains. Additionally pattern matching is required for identifying a dynamic model, and

for this multiple sources if data are used, including interviews, company reports, and reports by specialized agencies.

3.10.3 External validity

The external validity test is to establish how generalizable are the findings of the research (Saunders et al, 2016). The external validity is justified differently for each of the research processes followed:

- For the research about the nature of cyber-risks, multiple sources of data were used as part of the research design.
- For the research about systemic risk analysis, multiple cases were used as part of the research design, cases that are similar to an extent and thus comparable.
- For the case of the research about dynamic simulation, one case was used, which was analysed in depth, therefore aiming to be revelatory rather than generalizable.

3.10.4 Reliability

The reliability test deals with demonstrating that the process followed in the research can be repeated by different people with the same results (Yin, 1994).

The reliability is justified differently for each of the research processes followed in this thesis:

- For the research about the nature of cyber-risks, a study protocol was used for obtaining and analysing the data, and the data is kept in a database.
- For the research about systemic risk analysis, a study protocol was developed and the data collected in ways of the transcripts, is kept in a database,
- For the case of the research about dynamic simulation, a study protocol was used.

3.11 Methodology summary

This chapter described the need for a clear methodology as an essential part of this PhD thesis and gave a detailed description of the methodologies followed in this thesis work.

The chapter started by discussing the strategic aspects: the philosophical position taken throughout this study followed by the explanation of the approach to theory development chosen for this work, also known as the "logic" of the research. Thereafter the design aspects were discussed: the methods used for the research are explained and arguments for their choice were given. The chapter continued with an explanation of the strategies considered in the research, to then finalize by explaining the tactic aspects of this research, namely the data collection and data analysis methods for each of the research questions, and the considerations for the research quality were laid out.

After having presented the methodology upon which this thesis is based, this work describes the results from the application of these methodologies for answering the specific research questions.

4 Results: nature of cyber-risks

This chapter starts by providing background information about the justification for this part of the thesis research to then describe the gathered data.

4.1 Background

The systematic review revealed several knowledge gaps in the extant literature that make it difficult to answer the main research question directly. From a systems perspective, it is necessary to understand the underlying structure causing an "*unwanted behavior*" to only then define interventions to the system, either through policy or structural design.

For the case of cyber-risk and resilience in the global supply chain, the unwanted behaviour is the operational disruption derived from cyber-risks, and the underlying structures are the existing agents and connections in the system. A systems approach understands that it is through which this structure that disruptions occur. The more that is known about how those disruptions happen, i.e., the "*physics*" of the system (Sterman, 2000; Rahmandad, 2015), the better equipped an organization is to design a response and prepare for such an event.

However, the literature review revealed limited information about the way in which cyber-risks result in an operational disruption. Furthermore, the information that is available about

cyber-disruptions is circumscribed to the domain of IT and data transfer without the analysis of any resulting operational disruption. As a result, and as it is shown in the answer to RSQ 2 (see section 2.8.2) the limited information published about individual attacks gives rise to RSQ3.

This part of the thesis seeks to answer RSQ3 by gathering cases of cyber-attacks from sources beyond published literature to 1) obtain information about the structure of a cyber-attack and 2) provide information for evaluating the suitability of cyber-resilience methods to the nature, i.e., the particular characteristics, of cyber risks. The method that is followed is explained in section 3.7.

The following section describes the gathered data, which is further analysed in Chapter 7, section 7.1.

4.2 Data gathering results

The gathered data, in a similar fashion than the literature review, is first described and then discussed thematically.

4.2.1 Description of data

The initial gathered data consists in 2.425 events of cyber-attacks. As shown in Figure 40, no trend is detected in terms of the number of attacks over time. As this search is not exhaustive, this does not have implications on the number of attacks occurring

overall, and is only a description of the data that was gathered through the established protocol as per section 3.7 of this thesis.

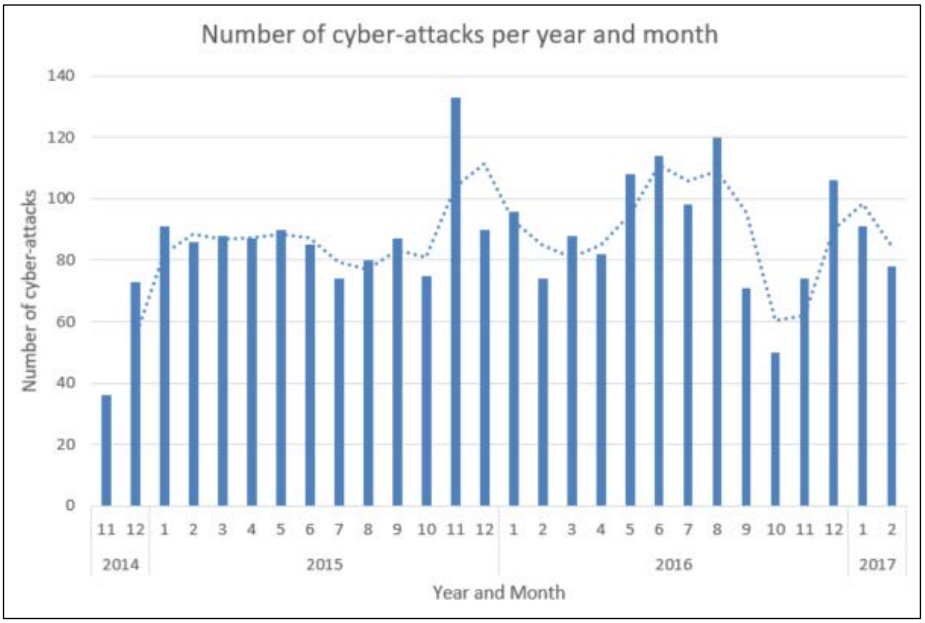

Figure 40 Number of gathered cyber-attacks

Two main indications have to be made about the reports represented in Figure 40: 1) Not of the cyber-attacks mentioned in the reports mention an effect on operations, and 2) the reports have multiple sources such as newspapers and blogs, independent blogs, specialist news boards and university news feeds. Table 23 shows a summary of the newspapers with the published reports of cyber-attacks considered in the data gathered.

Table 23 Distribution of reports by newspaper source

Newspaper	Percentage of articles
International Business Times	26,98%
The Register	19,07%
Reuters International	7,71%
BBC UK	5,07%
Forbes	4,87%
Bloomberg	3,04%
The Guardian	2,84%
BBC International	2,64%
The Independent	1,62%
Cnet	1,62%
New York Times	1,22%
Global News	1,22%
The Washington Post	1,22%
CBC	1,01%
New York Post	1,01%
Reuters UK	1,01%
ABC News	1,01%
Others	16,84%
Total	**100,00%**

The location where the attacks were directed is shown in Table 24. The country that present the most number of cyber-attack reports in the gathered data is the United States of America, with almost half of all the reports targeting organizations in that country.

Table 24 Target countries of cyber-attacks in sample reports

Target country	Percentage of attacks in data
United States	46,81%
United Kingdom	8,05%
India	3,96%
Canada	3,10%
Russian Federation	2,29%
Japan	2,11%
Australia	1,92%
France	1,30%
Israel	1,30%
Italy	1,30%
Thailand	1,24%
China	1,24%
Germany	1,24%
Korea (Republic of)	1,24%
Ukraine	1,11%
Sweden	0,93%
Others	20,87%
Total	**100,00%**

The process that is followed filters both according to the sources of data, and to the types of cyber-attack that are reported, to include those that have an effect on operations.

This filtering process is shown in Figure 41, and is based in the method described in section 3.7. The initial search process resulted in 2.425 reports of cyber-attacks from a wide variety of sources. By applying the criteria related to the source validity and the contents of the report, these reports were narrowed down by 60% to 950 reports. A further filter was applied to identify those reports that resulted in some form of operational disruption to consider information validity. The sources of the gathered

information are categorized and filtered according to the exclusion criteria in the research protocol. The detailed sample consisted of 5,7% of the narrowed down reports, which consists in 54 reports of cyber-attacks.

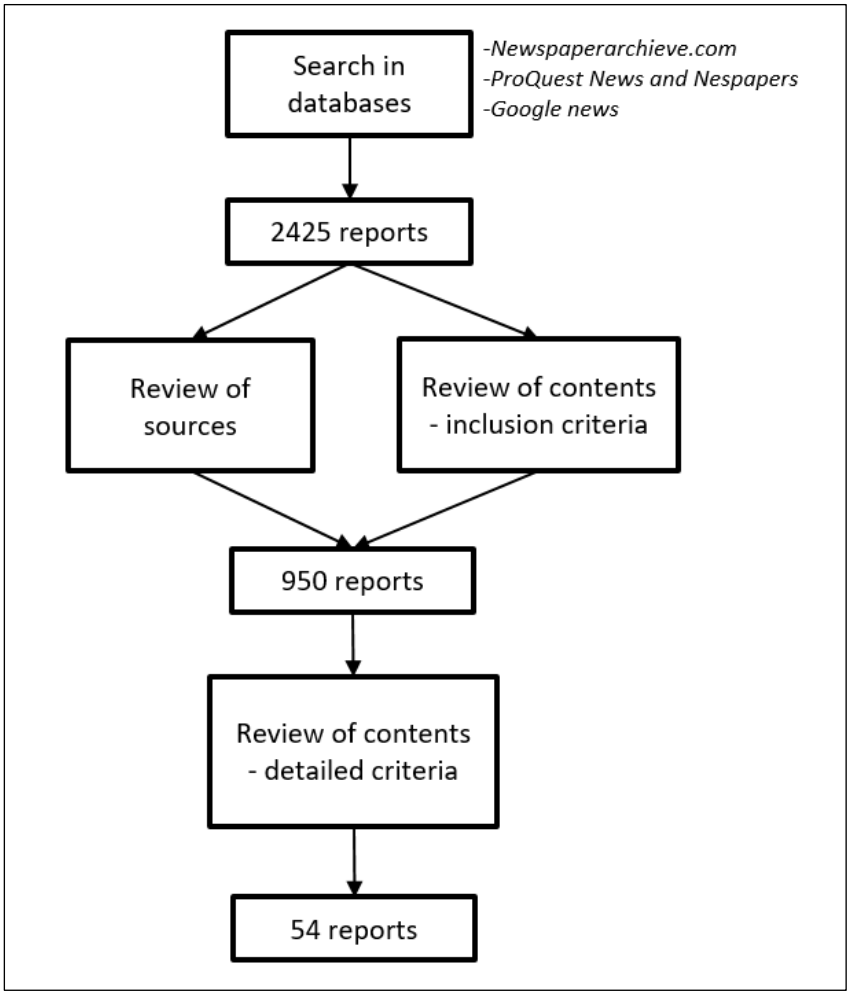

Figure 41 Report gathering process

The distribution of cyber-attack reports according to the different validated sources is shown in Figure 42.

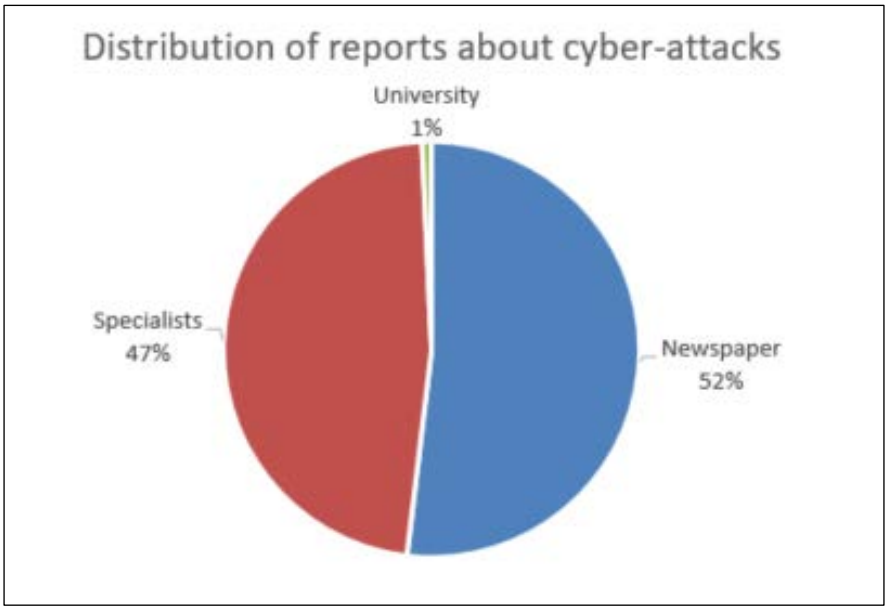

Figure 42 Distribution of reports about cyber-attacks

The analysis of the data proceeds by categorizing the cases according to their disruption effect.

Based to the definition by Christopher (2011) in section 1.3 of this thesis, a supply chain is a network of companies linked by activities that produce value in the form of products and services to a customer. As a result agents that participate in a supply chain have incentives to join in activities of value creation in the form of a products and / or services. This is illustrated in Figure 43.

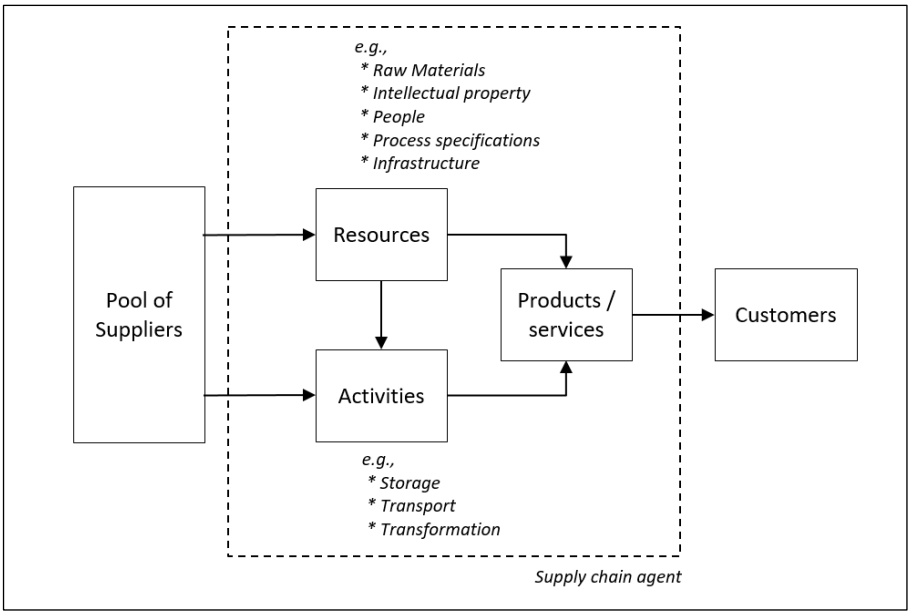

Figure 43 Supply chain agent (based in Christopher, 2011)

As a result, the areas where the supply chain agent can be disrupted generically are either related to the resources it has available, the activities it performs with these resources, and the products or services that contain the added value from combining the activities and resources.

As a result, the cases in the gathered data are organized and grouped according to the form that the disruptions in the cases took place. These groups are:

- Active theft of assets,
- Passive theft of assets,
- Active product theft
- Active interruption of operations, and

- Passive interruption of operations.

4.2.2 Active theft of assets

Theft of assets was a disruption type present in the data gathered. These cases occur in organizations that have the custody of some type of transferrable asset, and the data revealed cases in formal currency and in cryptocurrency (see glossary of terms) and digital intellectual property. It is active since the actions to create the disruption are executed by the hackers, not the target company.

Event description. The case of Tesco Bank[8] is descriptive of a form of cyber-risk that results in an "*active*" theft of money. In November 2016 Tesco Bank informed that 7% of all their customer's current accounts had been subject to criminal activity with the result that money was fraudulently withdrawn. Tesco bank's shares fell by 3% the day of the announcement. Initially, the bank did not disclose how much money had been stolen, but

[8] http://www.independent.co.uk/news/business/news/tesco-bank-cyber-attack-hack-25-million-pounds-hacked-bank-accounts-a7405591.html

https://www.thestreet.com/story/13882530/1/tesco-shares-drop-on-bank-hack.html

http://www.theweek.co.uk/78385/tesco-bank-cyber-attack-everything-we-know-so-far

https://www.thetimes.co.uk/article/tesco-hackers-used-mobiles-to-launder-haul-92tjftd57

http://www.bbc.com/news/technology-37974776

later informed that over £2,5 million had been paid out to over 9.000 customers as a result of the cyber-attack just two days after the attack had been acknowledged by the bank.

These attacks have been named by news reports as "*cyber-heists*".

The physics of the event. No unique explanation exists on the way in which the theft was carried out, as two main explanations have been put forward by the specialized news media:

- The first explanation is that, through previously stolen data hackers set up contactless payment accounts on smartphones, as revealed by the Sunday Times newspaper without identifying sources. In a coordinated action during the weekend when the theft was detected, thousands of purchases were made in Brazil and the US of low-priced goods by using smartphones; many of these transactions having been made to the US retailer Best-Buy. This assertion contradicts the original claim by the bank at the time of acknowledging the theft, that no personal customer information had been stolen.
- A second way was published by the Financial Times, and as source was cited an Israeli cyber-security company named CyberInt. This company indicates to have found evidence of Tesco bank customer information for sale in the dark web, reported by the BBC, information that was

obtained by "brute force", as the bank's website allows unlimited login attempts. This vulnerability allows an automated system to attempt different login combinations until one works out.

Similar attacks. Similar attacks have been experienced other institutions in different parts of the world, for example:

- The central bank of Bangladesh suffered the loss of more than US$ 101 million, in February 2016
- The Austro bank in Ecuador, suffered the loss of more than US$ 9 million,
- The central bank of Russia suffered the loss of more than US$ 45 million in December 2016,
- The Hong-Kong based cryptocurrency exchange service Gatecoin[9] suffered a cyber-attack in May 2016 suffering the loss of over US$ 2 million in equivalent Bitcoin and Ethereum.

Additionally, the theft of Intellectual property through cyber-attacks also appeared in the data.

[9] http://news.softpedia.com/news/gatecoin-bitcoin-exchange-loses-2-million-following-cyber-heist-504128.shtml

- In April 2016, US Steel made public the theft through cyber-espionage that had occurred in 2014 of strategic technical information that represented decades of research in creating the next generation high-strength steel[10]. The report indicated Chinese hackers as responsible.
- In December 2016, ThyssenKrupp a German industrial manufacturer revealed that a cyber-attack, probably originated in south-east Asia had stolen strategic project data, and they could not provide a "reliable estimation of the damage" as a result. The breach occurred in February 2016, and it was discovered in April of the same year[11].

Structure of the event. The structure of this type of operational risk can be represented by the interaction of the targeted organization and its immediate supply chain. Figure 44 shows the interactions mentioned in the descriptions of the normal operation of Tesco Bank.

[10] http://www.chicagotribune.com/business/ct-u-s-steel-china-alleged-hacking-20160427-story.html

[11] https://www.ft.com/content/7b556fb8-bd43-11e6-8b45-b8b81dd5d080

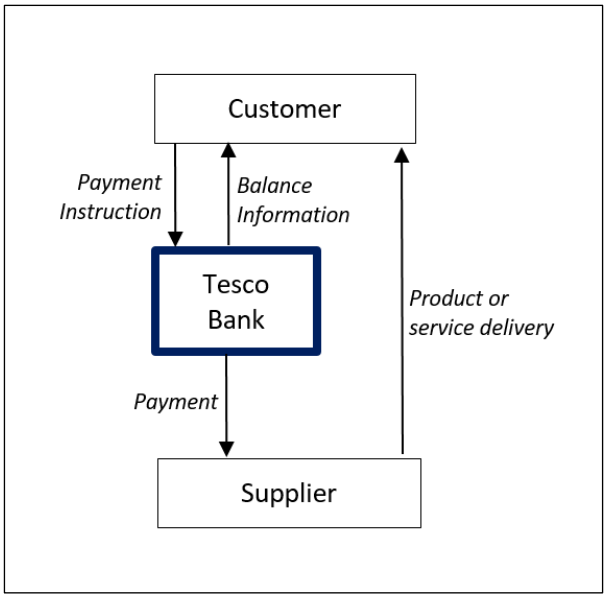

Figure 44 Pre-hacker diagram of active theft of resources

This diagram is a representation of the control structure, as described in the methodology of this thesis (see Figure 34 in page 253). The effect that hackers have on the operation of this system is both through the replacement of communications by fraudulent ones, or by influencing the system to generate an incorrect communication. The different diagrams components are represented in different ways in the control structure diagrams. These symbols are used in all the risk groups discussed in this section, according to the symbols shown in Figure 45.

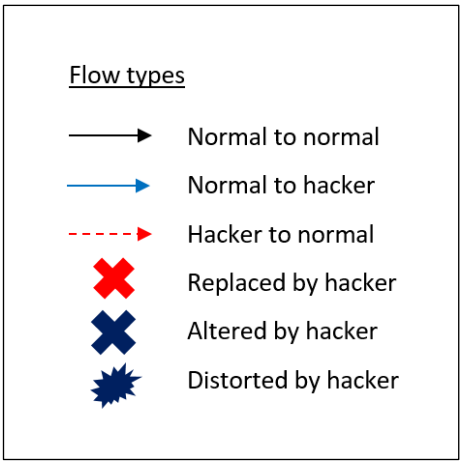

Figure 45 Symbols used in control structure diagrams

For the case of the active theft of resources, the effect of a hacker on the different flows is represented in Figure 46. This representation shows that the payment instruction from the customer, after a hacker intervention, has been replaced by a payment instruction from the hacker. The other effect is that the product or service is not delivered to the customer but to the hacker, despite the fact that the payment is still made to the supplier.

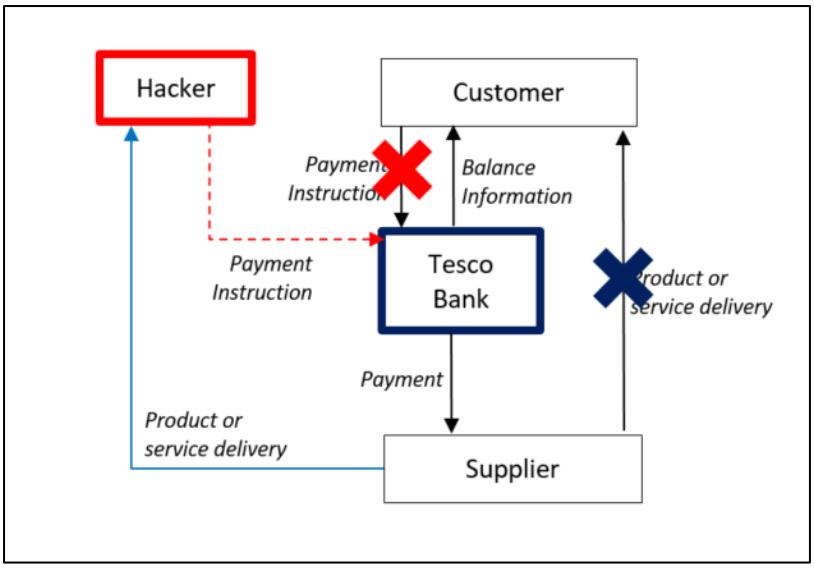

Figure 46 Post-hacker diagram of active theft of resources

The focus of the analysis is Tesco Bank (indicated in Figure 44 and Figure 46 with the thick-wall blue rectangle) and all hacker direct influences are shown in red. When the hacker is present and active, the normal payment instruction from the customer is replaced by a fraudulent payment instruction from the hacker. Tesco Bank, unable to tell the difference, proceeds with the normal payment to the supplier, e.g., Best Buy as indicated in the Tesco Bank example. The supplier as a result proceeds to deliver the product or service to the hacker instead of the customer.

This structure is equivalent to other case examples of passive theft of resources. For example, in the case of the Thyssen-Krupp intellectual property theft, a high level representation of the normal process is shown in Figure 47.

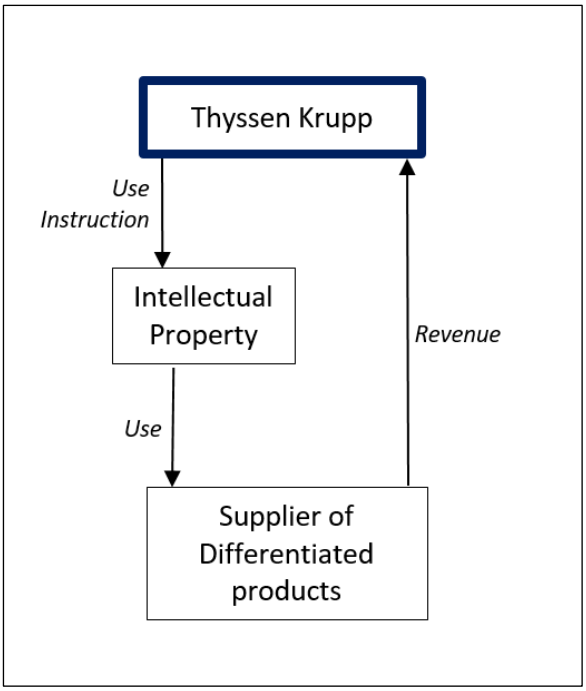

Figure 47 Thyssen-Krupp normal cycle of IP-Revenue

Figure 47 represents a normal cycle where the intellectual property of Thyssen-Krupp is used to generate a supply of differentiated products that result in a revenue for the IP owner. Thyssen-Krupp, as in the case of other industrial equipment manufacturers, do not normally manufacture all of the parts in their products, but rely on a market of suppliers who supply the products as per Thyssen-Krupp's specifications. The case with an active hacker present is shown in Figure 48.

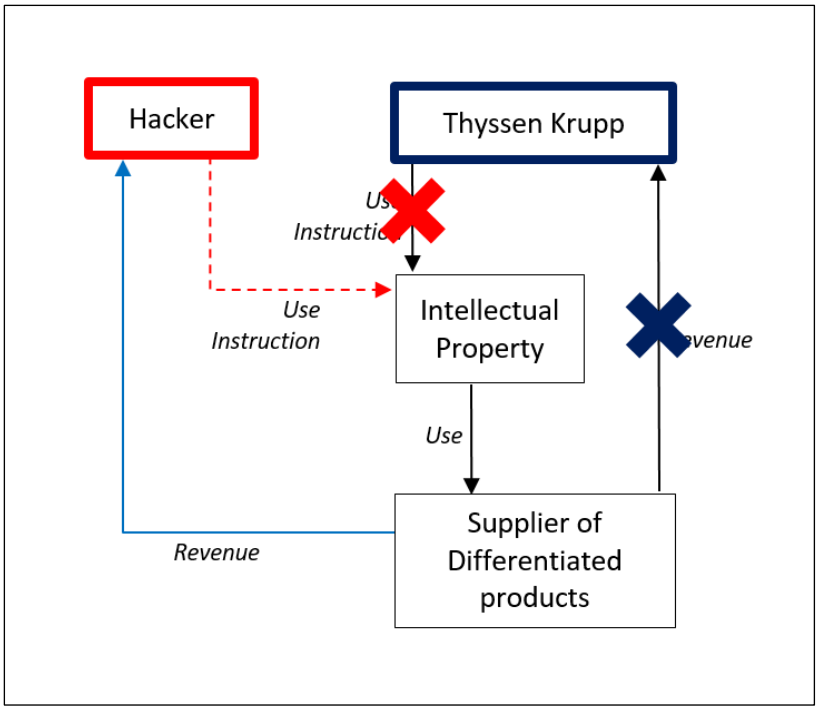

Figure 48 Thyssen-Krupp hacked cycle of IP-Revenue

The theft of IP is the equivalent of the hacker being able to issue the instructions of using these IP to the pool of suppliers to provide differentiated products and obtain the revenues. The cases of Tesco Bank and Thyssen-Krupp therefore, have a common structure that will be explored during the analysis.

4.2.3 Passive theft of assets

Some of the cases identified in the research that led to the theft of assets had an alternative sequence of events, where rather than hackers actively accessing target company systems, the hackers intervene the information used by the victims to carry out a process of transferring an asset. It is passive since the actions to

create the disruption are executed by the target company, not the hackers.

Event description. The case of Leoni AG[12] is descriptive of a form of cyber-risk that results in the "*passive*" theft of money. In august 2016 Leoni AG, Europe's biggest manufacturer of wires and electrical cables, and the fourth largest vendor of these products in the world, was tricked into paying over € 40 million (US$ 45 million) by electronic transfer to a fraudulent bank account. Leoni AG has over 75.000 employees in 32 countries around the world, and it celebrated 100 years of existence only one month after the attack. Its main customers are BMW, Mercedes-Benz and Rolls Royce.

When the company made the public announcement 4 days later (it is unclear when the mistake was detected), its shares fell 7%. This event happened in one of Leoni's manufacturing sites, specifically located in the city of Bistrita in Northern Romania. Of the four manufacturing sites owned by Leoni in Romania, only the Bistrita site has authorization to make payments, making this a directed attack.

[12] http://news.softpedia.com/news/one-of-europe-s-biggest-companies-loses-40-million-in-online-scam-507818.shtml

This attack has been named by news reports as CEO-Fraud, whaling or email spoofing.

The Physics of the event. The data reveals a unique version about the mode in which this fraud was carried out. The misdirection of funds was instructed through a fraudulent email sent from an unknown source to the Chief financial officer (CFO) of the company in Romania. The email was crafted to appear as if it had been sent by one of the top German executives of the company. Additionally, the fraudulent email contained inside information to appear more authentic, such as particulars about the company's transfer protocol, and the request followed company policy.

Similar attacks. Similar attacks have been experienced by other companies around the world, for example:

- In January 2016 the Austrian airplane parts manufacturer FACC lost over US$ 56 million through a similar scam[13].
- Also in January 2016, the Belgian bank Crelan (Credit Agricole) lost over US$ 75 million in similar circumstances to the FACC case.

[13] http://news.softpedia.com/news/company-fires-ceo-after-falling-victim-56-million-online-scam-504519.shtml

- In March 2016, Mattel was scammed in to paying US$ 3 million to an unidentified destination in China.
- The Brisbane city council in Australia lost US$ 500k to scammers in August 2016[14] .

The FBI has recorded at least one victim for this type of attack for every US state, along with victims from other 100 countries, with money being sent fraudulently to 79 countries. The most frequent destination for fraudulent payments is China and Hong Kong (FBI, 2016).

Structure of the event. The structure of the event has differences with the structure presented in the previous case group. In the case of a passive theft of resources. The Leoni AG case is represented by a control structure diagram as shown in Figure 49. The CFO orders a payment from the bank to the supplier after an instruction from the CEO, and a product is delivered to the warehouse.

[14] http://www.theregister.co.uk/2016/08/16/brisbane_councillors_lose_500k_to_scammers/

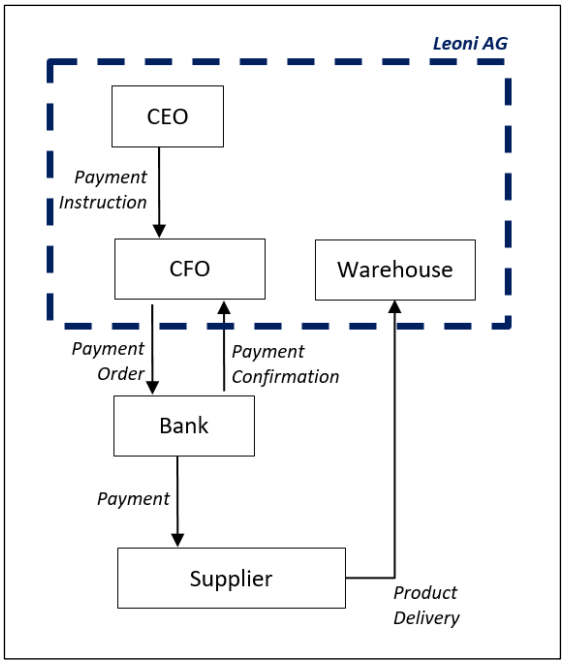

Figure 49 Leoni AG case pre-hack

The altered structure when a hacker is present, is represented in Figure 50. The flows are represented according to the symbols indicated in Figure 45. The effect of a hacker is the replacement of the communication from the CEO to the CFO with a fraudulent communication from the hacker to the CFO. The effect is that the bank issues the payment inadvertently to the hacker instead of the warehouse.

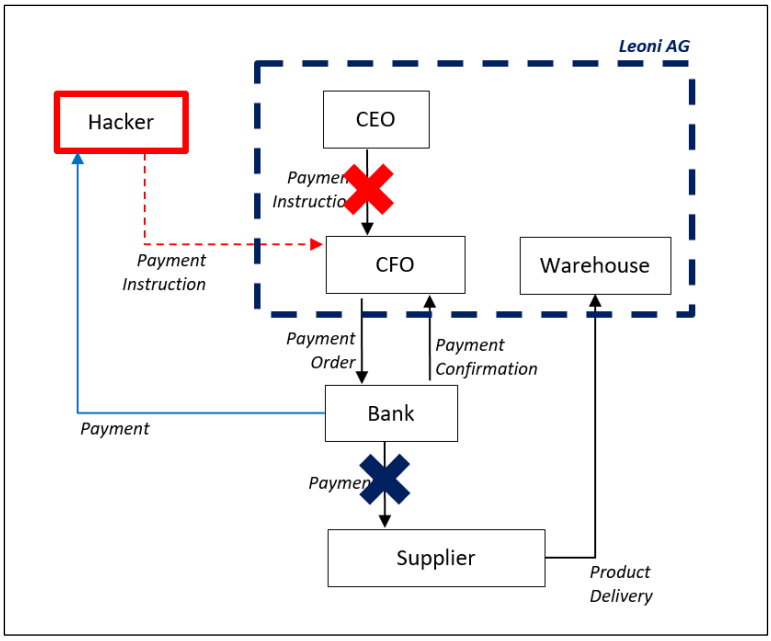

Figure 50 Leoni AG case post-hack

An interesting effect of this type of case, and in contrast with the active theft shown previously, is that it is partners upstream that are affected by this attack, as the supplier, having delivered the product, do not receive timely payment. In contrast, in the case of the active theft of resources, it is the customers, and therefore the downstream supply chain, that experience the effects of the cyber attack.

4.2.4 Active product theft

The attacks described in the previous sections have different effects in the supply chain. An active money theft, being bounded to the resources owned by the target organization, does not affect suppliers or customers. On the other hand, passive money theft

can potentially affect suppliers by misdirecting payments as the cases in the previous section illustrate. Another type of cyber-risk found in the data affects customers, in the form of misdirecting, and thus stealing, products through an active participation of foreign agents. It is an active attack as the actions to create the disruption are executed by the hackers.

Event description. The case of the Hyundai and Kia cars is representative of an active product theft. In December 2016, product and customer data that had been stolen from Hyundai and Kia in Israel, was used by a network of criminals to steal dozens of cars and smuggle them to the West Bank[15].

The physics of the event. A network of criminals used a list of car identification plates to locate the vehicles in the city. When one was found, the data was used to identify both the code of the keys, of which a copy was made, and the address of the owner, from where the car was stolen.

Similar attacks. Other active product theft examples were identified in the gathered data, for example:

[15] https://www.scmagazine.com/alleged-car-thieves-used-breached-data-to-help-steal-hyundais-and-kias/article/580425/

- A cyber-attack has been recorded in the UK for the theft in 2016 of BMW luxury cars that have the key-less feature[16].
- An unnamed global shipping company[17] experienced an attack in 2016, where by using stolen data obtained from a previous network intrusion, pirates had specific knowledge at the time of boarding a vessel, and located specific containers through the bar codes and steal the contents of that crate.
- Another case of active product theft in Manchester, UK in 2015[18] did not require network intrusion, but instead disrupted the signal, i.e., "jammed the signal", of the remote lock for all the cars in a parking lot. This led to some drivers not being able to open or close their cars, and set off alarms uncontrollably. Despite the many implications of such a simple but effective attack, no product loss was reported.

Structure of the event. In the case of the KIA and Hyundai car thefts, the structure of a normal process is represented in Figure

16 http://www.dailymail.co.uk/news/article-4456992/Shocking-moment-car-hackers-steal-60-000-BMW.html

17 https://arstechnica.com/information-technology/2016/03/pirates-hack-into-shipping-companys-servers-to-identify-booty/

18 http://www.theregister.co.uk/2015/05/20/car_park_vehicle_locks_hacked_en_masse

51. This is a simple representation of the normal interaction between a product and its owner through some type of control system by using proprietary information, which in the case of the stolen cars is the key codes and address. Other examples of proprietary information include the electronic key code and medium for the case of the keyless BMW cars, and the container contents and ship location in the case of the global shipping company case.

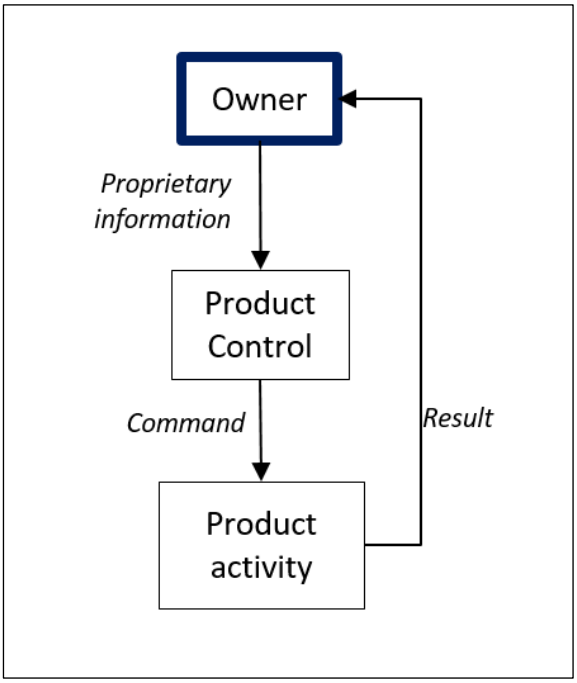

Figure 51 Kia and Hyundai car normal process representation

When the hacker is present, the proprietary information is used by the hacker to obtain results from the control system, as shown in Figure 52. The flows are represented according to the symbols indicated in Figure 45.

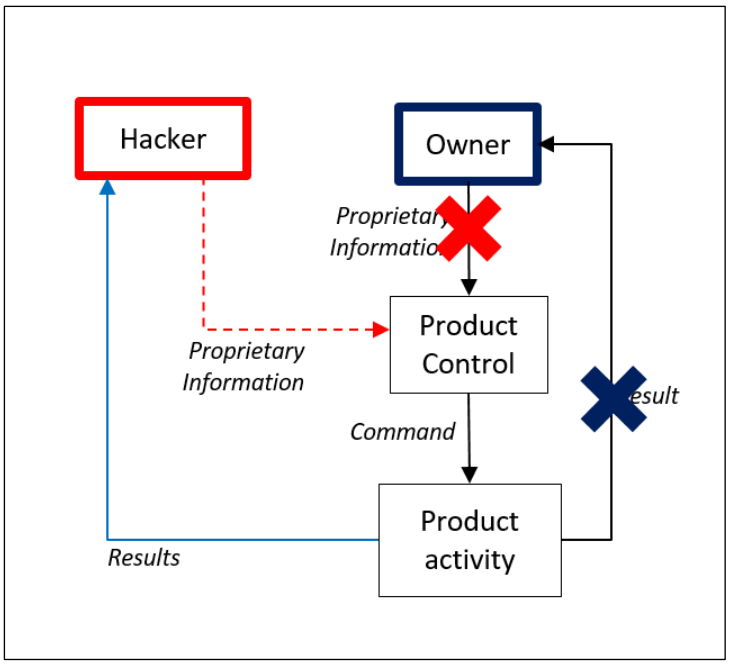

Figure 52 Kia and Hyundai car hacked process representation

By accessing the control system of the cars and the physical location of these cars, the hackers can obtain results of a normally functioning control system and car, instead of the owner.

4.2.5 Active interruption of operations

Some cases in the gathered data relate to the interruption of productive operations as a result of a cyber-attack. It is an active attack as the actions to create the disruption are executed by the hackers. It is active since the actions to create the disruption are executed by the hackers, not the target company.

Event description. The case of a German steel manufacturer is representative of a cyber-attack affecting operations. In late 2014

a steel mill was the subject of a cyber-attack through which unidentified foreign agents disrupted the production process[19]. This attack made public by de German federal office for information security, known as BSI (Bundesamt für Sicherheit in der Informationstechnik). BSI describes it as the second disclosed case in the world of a cyber-attack causing physical damage after Stuxnet in 2010. As a consequence of the intrusion, one of the plant's blast furnaces was shut down in an uncontrolled manner, resulting in massive damage to the plant.

BSI indicates that perpetrators of this attack have not been identified, yet the structure of the attack could only have been designed by a group people knowledgeable about industrial control systems. No motivations have been identified either for this attack.

The physics of the event. The BSI did not disclose the location or the name of the company that was affected, but revealed the process through which the disruption was executed.

- The hackers access the office software network of the industrial plant, through what is known as "*spear phishing*",

[19] https://www.sentryo.net/cyberattack-on-a-german-steel-mill/ https://www.wired.com/2015/01/german-steel-mill-hack-destruction/

similar to the hacking process described in the passive money theft, a fraudulent emails that seem to come from a legitimate source encourages the recipient to open an attachment or visit a website that contains a malware.

- From the office software the hackers penetrate the steel mill production management software,
- Hacker take over most of the plant's control systems
- Hackers methodically destroyed human-machine interaction components
- Hackers prevent blast furnace from initiating its security settings at the correct time
- Incorrect operation caused damage to physical infrastructure

Given the complex attack sequence and the prolonged time through which the attack is materialized, these attacks have been denominated as Advanced Persistent Threats, or APT.

Similar attacks. Different examples of cyber-attacks similar to the one described for the steel mill were found in the gathered data.

The most famous cyber-attack that resulted in physical infrastructure damage is the Stuxnet worm, detected in 2010. This attack is found as part of the SLR process to answering RSQ 2 (see section 2.8.2). Stuxnet is a computer worm targeting nuclear enrichment facilities, and is suspected to having had different

versions released to the internet, as far back as 2006. Stuxnet affects the control of the centrifuges, an equipment central to the process of uranium enrichment. By tricking the control system, Stuxnet led centrifuges to spin far above their recommended speeds, causing them to fail (Zetter, 2014). Stuxnet has several distinctive features, such as:

- It is a directed computer worm with an attack sequence in three phases: 1) first it seeks out computers in the network running Microsoft Windows, then 2) seeks out a specific Siemens programmable logic controller (PLC) connected to that computer, to then 3) alter the controlling software for this PLC to influence the control of the underlying process of uranium enrichment.
- The disruption process it caused was autonomous and did not require a connection to the Internet to function.
- Stuxnet used proprietary keys and undiscovered software vulnerabilities, i.e., zero-day vulnerabilities.

Research into this malware was carried out through the gradual unencrypting of a particularly large file of code discovered in the infected computers. This unencrypting resulted in the discovery of an extremely sophisticated program with characteristics that led experts at the time to characterize it as the first "*cyber weapon*" (Zetter, 2014).

Not all cases of active interruption of operations resulted in equipment or infrastructure damage as a result of the cyber-attack. Examples of infrastructure and equipment foreign intervention and control as a result of a cyber-attack include:

- In 2013, hackers took control of the control systems of a New York dam[20]. The attackers were not able to open the gates only because the gate had been manually disconnected for maintenance at the time of the attack[21].
- In March 2016, an unnamed water treatment plant was hacked[22]. Hackers took over the control systems and changed the levels of chemicals used to treat tap water.
- In December 2016, several electricity cuts affected Turkey, caused by cyber-attacks[23], and affecting industrial regions from Kocaeli to Istanbul. A similar attack to interrupt electricity delivery occurred in Ukraine in 2015[24]. These attacks are normally carried out by hackers taking over the

[20] http://www.theregister.co.uk/2015/12/21/iranian_hackers_target_new_york_dam/

[21] http://time.com/4270728/iran-cyber-attack-dam-fbi/

[22] http://www.theregister.co.uk/2016/03/24/water_utility_hacked/

[23] http://www.hurriyetdailynews.com/major-cyber-attack-on-turkish-energy-ministry-reported.aspx?pageID=238&nID=107981

[24] https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/

control systems to disconnect switches, thus cutting the supply of electricity to whole regions.

- In 2014, a floating oil rig from an unnamed company was taken over by hackers who tampered with its control systems, tilting it to the point where the production had to be shut down. It took 19 days to make the structure and control systems sea-worthy again (Wagstaff, 2014).

Structure of the event. The active interruption of operations case of the steel mill before the hacker attack is represented in Figure 53.

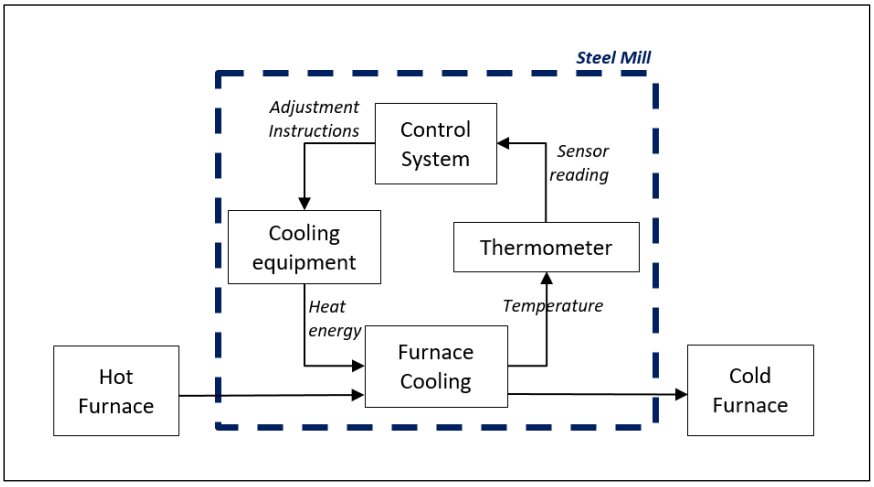

Figure 53 Steel mill process pre-hack

In a normal steel mill cooling process, the input is a hot furnace that through the furnace cooling process, results in the output of a cold furnace. This cooling process is controlled by the continued interaction between sensors that measure the state of the process, in this case thermometers that read the furnace temperature, and

the actuators that influence the process, in this case the electric arc generators which create the heat and coolers that take heat away. The control loop that is illustrated in Figure 53 represents this interaction as mediated by the control system, which directs the net heat production from heaters and coolers as a result of the temperature signalled by the thermometer, and according to a cooling algorithm contained in the control system.

A hacker that disrupts this process, may do it to take it over or to disrupt the normal activity. The intention of the attackers has not been informed. Yet, according to the reports, the result of the cyber-attack was an uncontrolled cooling of the furnace, and as such, can be interpreted as disruption of activity. This is represented in Figure 54. The flows are represented according to the symbols indicated in Figure 45.

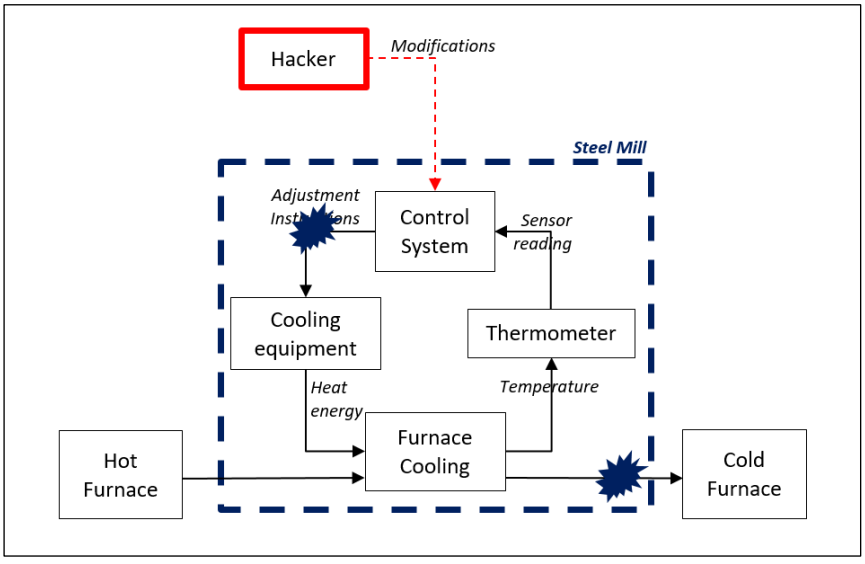

Figure 54 Steel mill process post-hack

The effect of the modifications by the hackers to the control system is a distortion of activities and communications in the cooling process. By altering the decision algorithm, the action to the heat generators or coolers that can lead to equipment damage such as inner lining destruction or excessive hydration of steel furnaces (Verscheure et al., 2006).

4.2.6 Passive interruption of operations

Several of the cases in the gathered data described an unexpected interruption of operations executed by the organization target of the cyber-attack, i.e., a passive interruption, which presents a different structure and sequence of events leading to the physical disruption.

Event description. The Wannacry ransomware attack in June 2017 and its effect on the national healthcare system (NHS)[25] is an example of a passive interruption of operations. The infection by this ransomware infected more than 150.000 computers in 150 countries, and in the case of the NHS the ransomware resulted in the interruption of service in different hospitals of the system, the

[25] https://www.nbcnews.com/news/world/why-wannacry-malware-caused-chaos-national-health-service-u-k-n760126

rejection of patients, the treatment of patients without their digital health records or prescription dosages, the derivation of patients to other parts of the system, and the rerouting of ambulance services. No perpetrator or motives for the attack have been identified. The NHS indicated that at least 16 of its organizations were affected by the Wannacry ransomware[26].

The physics of the event. Incident researchers agree on the sequence of events that leads to the operational disruption.

- From an already infected computer, the Wannacry worm actively looks in the network for computers with a Windows operating system
- When a computer is found, Wannacry exploits a software vulnerability called "EternalBlue" to infect this computer.
- Computers infected by Wannacry unexpectedly request from the user a restart, proceeding to encrypt most information in its hard drive. The only folder not to be encrypted was the Windows folder.
- Upon restarting, Wannacry displays a message requiring the transfer of US$ 300 to US$600 to a specific bitcoin account. The message proceeded to read that decryption key would

[26] http://www.npr.org/sections/thetwo-way/2017/05/12/528119808/large-cyber-attack-hits-englands-nhs-hospital-system-ransoms-demanded

then be sent to release the data. The message screen is illustrated in Figure 55.

Figure 55 Wannacry message screen

- The encrypted information included patient data, and hospital schedules, for example.
- This sudden lack of information leads to palliative measures such as the rerouting of ambulances to other organizations in the system, the rejection of non-urgent new patients, or the treatment of patients without their healthcare record.

Similar attacks. Other similar attacks have occurred, and this Wannacry attack has also affected other industries.

- A ransomware attack, named "Petya" affected operations at the nuclear plant in Chernobyl, Ukraine in 2017. No

equipment was destroyed due to the attack, but energy production was interrupted as a preventive measure, as vital metrics and reports were not accessible on the computers during the attack[27].

- In 2013 a ransomware named Cryptolocker infected over 500.000 computers around the world demanding US$ 300 in Bitcoin to the victims to release the encrypted files[28].

Structure of the event. The operation of the NHS can be represented by a control structure as illustrated in Figure 56. A doctor determines actions in a treatment process to a patient, to convert an incoming patient to a treated patient. The doctor is equivalent to the "controller", who has an internal set of decision rules, i.e., the medical algorithms, and the data of the patient. The data is collected through the measuring of the patient's biometrics, in an ongoing process.

[27] http://www.express.co.uk/news/world/821971/Chernobyl-nuclear-power-plant-hit-ransomware-cyber-attack

[28] https://www.theguardian.com/money/2013/oct/19/cryptolocker-attacks-computer-ransomeware

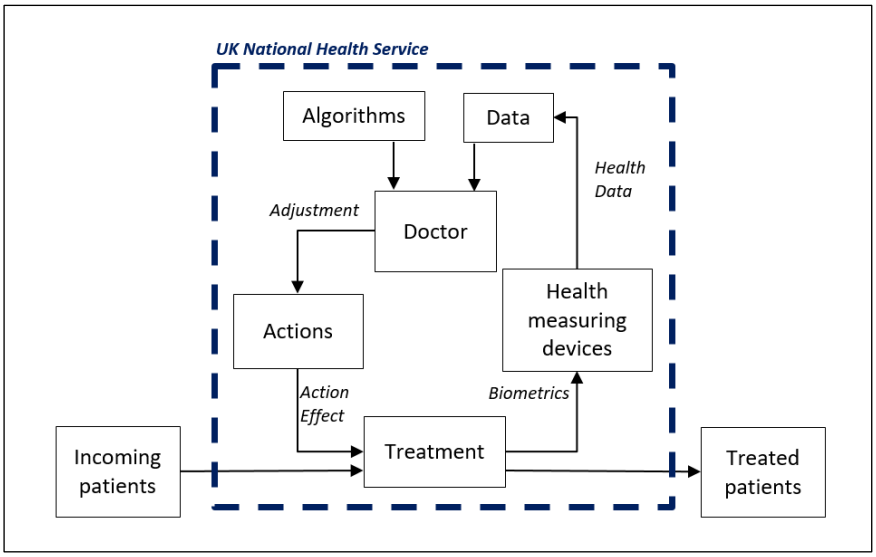

Figure 56 NHS process representation pre-hack

The passive interruption of operations as described for the Wannacry ransomware attack affected the operations of the NHS blocks the access to data, as illustrated in Figure 57. The flows are represented according to the symbols indicated in Figure 45.

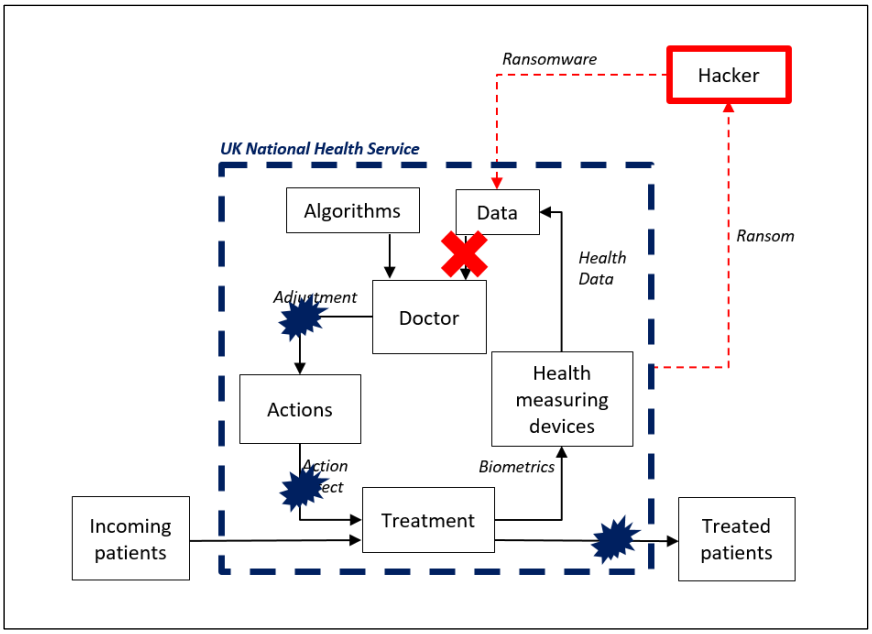

Figure 57 NHS process representation post-hack

The Wannacry ransomware, by making data inaccessible to the controller, i.e., the doctor, causes a distortion in the adjustment calls and as a result in the effects of these action calls. As a result the treatment process has a distorted outcome.

4.3 Summary of the chapter

This chapter started by providing background information about the justification for this part of the thesis research to then describe the gathered data.

The analysis of this data is presented in chapter 7. The next chapter describes the results from the systemic risk analysis process.

5 Results: systemic risk analysis

This chapter describes the results of using the systemic risk analysis method STPA to the analysis of cases of organizations exposed to cyber-attacks. It starts by giving a description of the case where this method was applied. The chapter ends by describing the results that were obtained from the STPA application.

5.1 Case description

The case company is a beverage manufacturer based in the United States of America with manufacturing operations in 23 countries. This company has a complex supply chain and has a distributed, global supply team that procures raw materials and packaging to all operations through a regional structure. Particularly in the Americas this company has 7 manufacturing sites and its regional structure since 2007 has been a matrix distribution of raw material purchasing responsibility, where a procurement team in each of the locations is responsible for the purchase of a number of materials for all the other locations in the region, in what has been called a "*Virtual Organization*" (VO) of procurement. The procurement team is therefore considered as a regional, America-level team. A general representation of the manufacturing sites in the Americas is shown in Figure 58. It is important to consider that only the procurement team is managed

at an America-wide level, and all other aspects of the different plants are managed individually.

This company launches as many as 70 new products per year, has a 99.5% operational service level requirement, and implemented a version of the Lean methodology both to its operations and to its service areas in the company, with varying degrees of success.

The products that are purchased by this matrix organization include raw materials in solid and liquid form, and some types of packaging, as most of the packaging is purchased locally by each plant (mainly plastic containers and cardboard boxes).

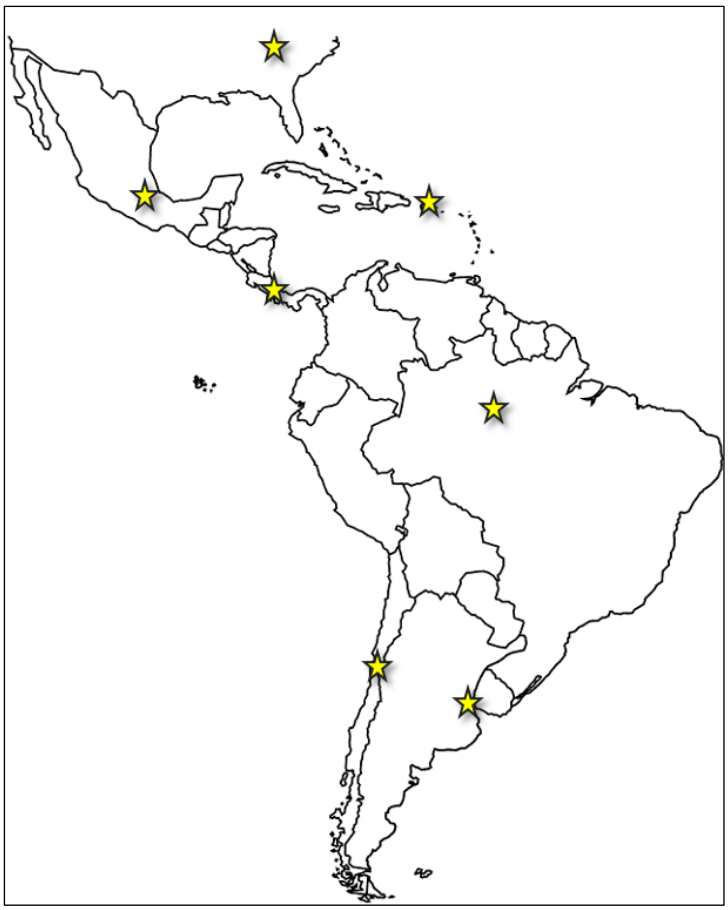

Figure 58 Beverage manufacturer production sites in America

From this structure, every world region has a relationship with local suppliers in the case of packaging, and global suppliers for the case of raw materials. Global supplier conditions are managed centrally in the US headquarters on an annual basis, while regional the regional supply VO manages the daily operations with these suppliers.

As part of a strategic goal of implementing safe, reliable operations, this company is particularly interested in

understanding the exposure they have to cyber-risks, as they are sensitive to public opinion and reaction in the case they were to be attacked: nearly 63% of its market value is related to intangible assets, such as trademark, patents, and trade dresses. For more information on intellectual property, see section 6.1.

This company has detailed procedures. In particular, risk is identified through a detailed, standardized risk analysis process. The main tool that is used is the Failure Mode and Effects Analysis (FMEA) method, particularly for the operations area, within the framework of the Supply Chain Operations Reference framework (SCOR) for the SCM area.

The Supply Chain Operations Reference (SCOR) is a framework that was developed by the Supply Chain Council with its first version published in 1996, and is currently developed by APICS, the American Production and Inventory Control Society (Ntabe et al., 2015). It is based on the analysis of five distinct management processes for every agent in the supply chain, namely Plan, Source, Make, Deliver and Return (APICS, 2010). For a supply chain, there is a planning process over the supply chain units, as is represented in Figure 59.

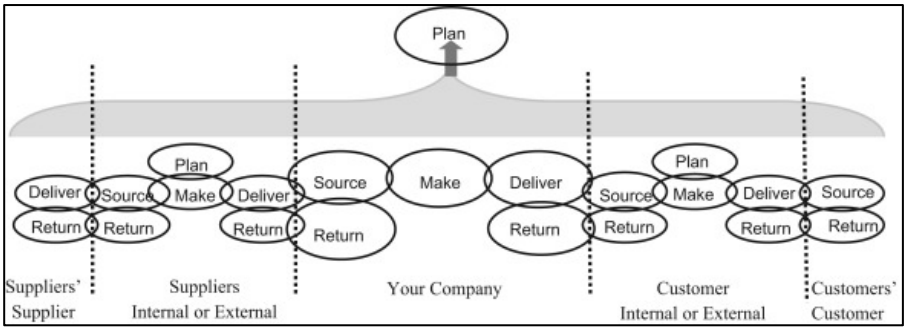

Figure 59 SCOR model (APICS, 2010)

The SCOR framework makes no reference to cyber-risks up to its version 10 (2010) and Value at Risk (VaR) as the main indicator for other risks in the supply chain. The VaR is calculated normally through a process of FMEA.

The FMEA process is executed by identifying the elements that are part of the system, and identifying the ways in which these elements can fail, as well as the severity of the effects if these failures were to happen. This company considers probability of occurrence in categories, namely “very unlikely”, “somewhat unlikely”, “somewhat probable”, “very probable” and “extremely probable”. The Value at Risk is calculated as the sum of the consequences of all risks that have a probability of “probable”, “very probable” or “extremely probable”.

These values, i.e., the identification of the modes of failure, the probability of occurrence categories and the severity of the events occurring, are identified in workshops with the participation of members of the organization from warehouse, procurement,

expediting, quality, finance, production and maintenance. For the Americas plants, these processes have used as few as 8 and as many as 15 people per meeting, with a total use as many as 240 man-hours of meetings (4 meetings of 4 hours each for 15 people) plus processing time of another 20 hours by the risk analysis team.

Since FMEA is a reference framework with no set indications on how to measure, probability of failure, severity of failure or identification of the failure modes, the process is highly dependent on the experience of those taking part in it. The whole process is carried out every year, mainly as an update of the previous year's FMEA results, and normally a set of preventive and mitigation measures are identified with action owners. These actions are followed up in monthly meetings.

As a part of their yearly risk assessment process, this company updates, at an America level, its risk analyses for all plants and processes, with a special focus on including cyber-risks within the analysis for the year 2016. Their process is carried out through the usual FMEA process. Supply managers at three of the plants agreed to participate in a pilot test of the STPA process to be run in parallel, and to compare the results of these processes with the results delivered by FMEA. The management team at the case company had detected different problems with the current risk assessment method, such as:

- The rotation of experienced personnel had been increasing over the last 10 years, and it was highly likely that this would continue. This was mainly attributed to a "generational changeover" being experienced by the company, as it was likely to find people with over 15 years of experience. Management had its reservations of being less dependent on the experience of people by using a risk analysis method that was less history-dependent,
- The company had not experienced cyber-attacks yet, but its management continues to be highly sensitive to problems derived from public image problems, and cyber-risk was thus high in their agenda,
- The company had implemented the Virtual Organization (VO) and before going beyond procurement, wanted to understand communication risks and potential interventions derived from cyber-risks,
- The risk numbers, particularly related to severity of the failure modes had increased little over the years if at all, in a wat that had no relationship to any other indicator in the company. As such, management had the impression that those numbers were not being reviewed and were just being adopted from the previous year's report.

In order to develop the process in detail, the procurement process was chosen for the analysis and subsequent comparison.

5.2 Results of STPA application

The process that is followed for developing this STPA analysis is explained in detail in the methodology section 3.8.

According to the systems engineering approach (Leveson, 2011), the required start is by identifying a system goal to be achieved. A typical purchase transaction consists of a set of interactions between a buyer and a seller for the timely delivery of a product at the agreed price to the buyer through the use of a transport agent. The process begins when the buyer sends a purchase order to the seller, and ends when all involved have been paid and the product has been successfully received. Therefore the goal of procurement was defined as:

"*A system to safely and timely purchase the correct product by means of an cost-effective relationship with our supplier and their transport, in order to contribute to the company's bottom line and reputation*"

From this definition, a set of unacceptable accidents were agreed with the participants in the workshops, losses which are aligned to the objectives of the company and of the procurement process itself. These are denominated "accidents" and are shown in Table 25.

Table 25 Unacceptable accidents / losses

A1	Erroneous arrival of product
A2	Erroneous payment to supplier
A3	Product loss
A4	Product integrity compromised
A5	Payment Loss
A6	Reputational Loss

Additionally, the hazardous situations were identified, that would lead to a loss, as indicated in Table 26.

Table 26 Hazards in the system

H1	Inability to initiate supply process
H2	Inability to perform physical transport
H3	Inability to confirm product integrity
H4	Inability to confirm correct payment
H5	Inability to confirm data integrity
H6	Inability to confirm data transmission integrity

The process steps have been defined by the company's procedures, and these are represented in Figure 60.

Figure 60 Process diagram

Additionally, for the process of procurement, the controllers that take part in the process have been identified as the Plant, the Supplier, the transport agent, the plant's bank and the supplier's bank. To carry out the process required by the procedures, and as represented in Figure 60, each controller is in charge of executing a series of actions, the Control Actions required for the process. These are shown in Table 27

Table 27.

These control actions can also be represented in the hierarchical control diagram by considering controllers, control actions and hierarchy. Controllers that are placed higher up in the diagram have more control over the system's goals and function, as they have the capacity of affecting the actions of controllers below them. Figure 61 illustrates this for the system under consideration. The plant is the controller with the highest hierarchy, as it is in the plan that the procurement goals are defined, and where the activities of all the other controllers can be influenced. On the contrary, the transport, does not control the goals and objectives of the system, rather reacts to the control actions of other controllers, and its control actions only are confirmations (passive responses). Its only active control actions are the pickup from the supplier and delivery to the plant.

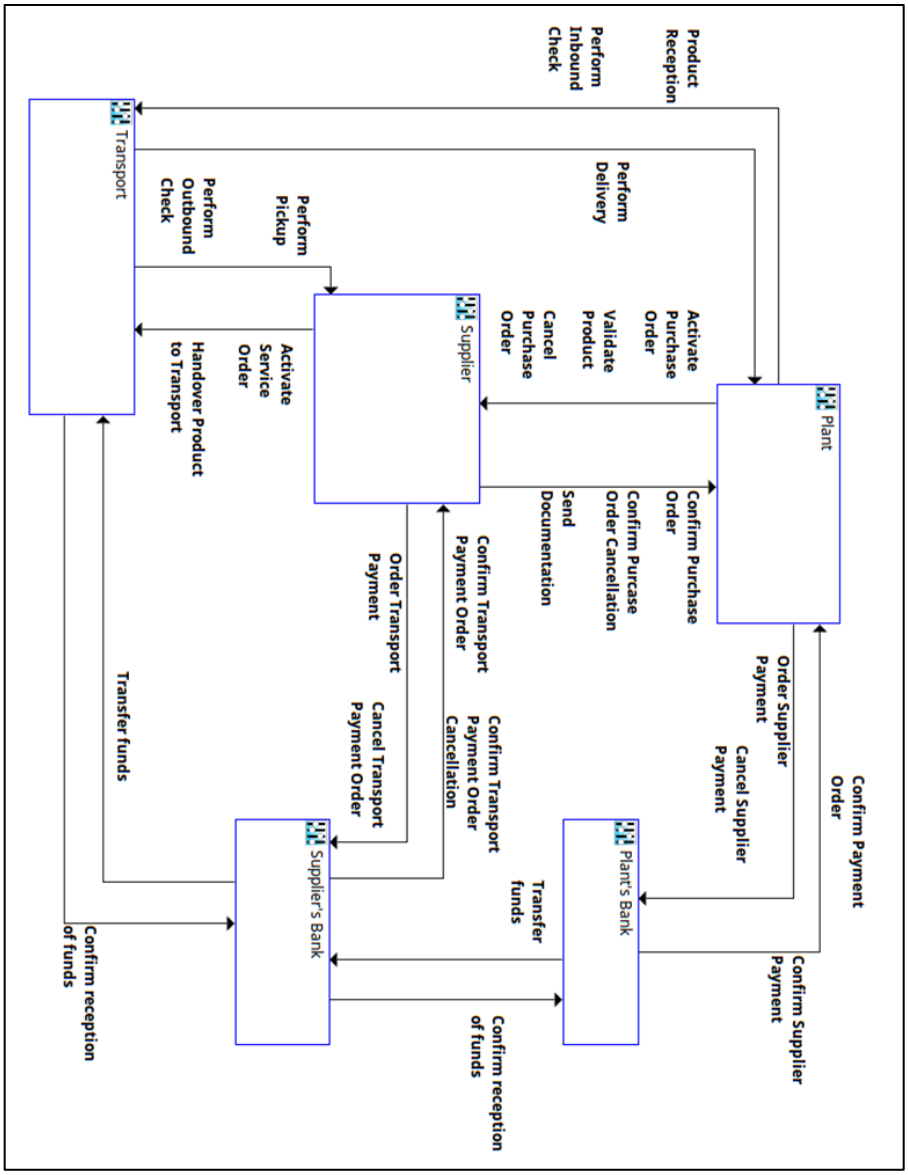

Figure 61 Hierarchical control structure

Table 27 Process-controller matrix

		Controllers				
	Control Actions	**Plant**	**Supplier**	**Transport**	**Plant's Bank**	**Supplier's Bank**
Process Steps	**Order**	*Activate Purchase Order *Cancel purchase order	*Confirm purchase order *Confirm purchase order cancellation	-	-	-
	Prepare	-	*Activate service order *Cancel service order	*Confirm service order activation *Confirm service order cancellation	-	-
	Outbound Check	-	*Handover products to transport *Handover transport documents to transport	*Perform outbound check	-	-
	Pickup	-	-	*Perform pickup	-	-
	Transport	-	*Send documentation	*Perform delivery	-	-
	Inbound Check	*Perform inbound check	-	-	-	-
	Receive	*Receive product	-	-	-	-
	Validate	*Validate product	-	-	-	-
	Pay	*Order supplier payment *Cancel supplier payment	*Order transport payment *Cancel transport payment	-	*Confirm supplier payment order *Confirm supplier payment order cancellation *Transfer funds to supplier	*Confirm transport payment order *Confirm transport payment order cancellation *Transfer funds to transport

According to the process detailed in Figure 35, the system and its goal has been identified, as well as the hazards, control actions and unacceptable losses. The next step is to identify the ways in which the control actions can influence the system into getting

into a hazardous condition that might lead to an unacceptable loss. For this, a matrix is used to identify for each of the control actions, its four potential unsafe modes: 1) the application of a control action leads to a hazardous condition, 2) the non-application of the control action leads to a hazardous condition, 3) applying the control action too early or too late leads to a hazardous condition, and 4) applying the control action for too long or too short a time leads to a hazardous condition. Figure 62 shows an extract of the analysis as it was done through the XSTAMPP software.

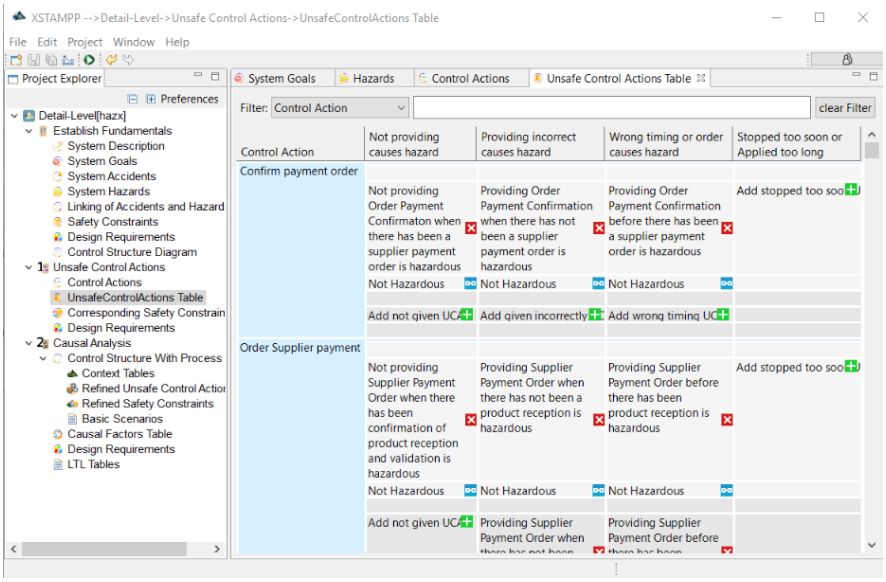

Figure 62 UCA Analysis through XSTAMPP software

In total 119 unsafe control actions (UCA) were identified. Of these the number of hazards that was associated with each UCA ranged from two to five, as shown in the next graph:

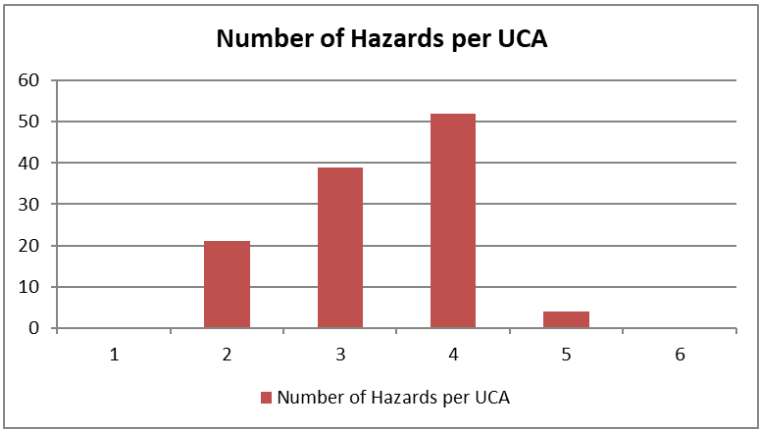

Figure 63 Number UCA per number of associated hazards

Of the UCAs that were identified, 37% corresponding to actions that had an incorrect timing, 45% of them considered an incorrect action being executed, and in 18% of the cases the control actions were not given as can be seen in Figure 64.

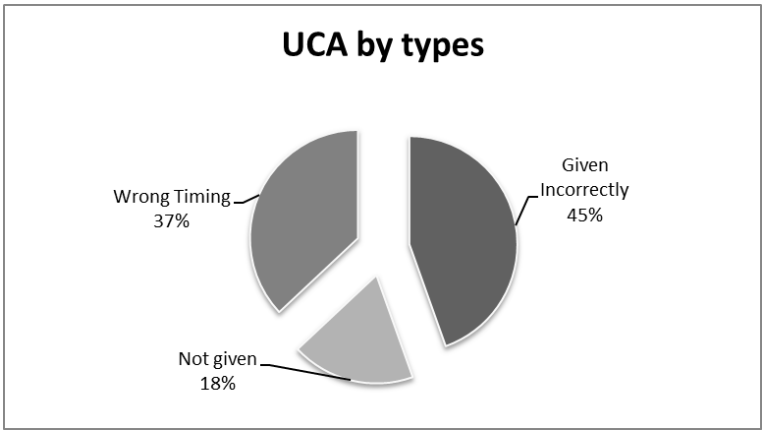

Figure 64 UCA by type

Examples of each type of UCA is shown in the next table. The complete list of unsafe control actions can be found in appendix

11.2, and Table 28 shows a summary of the STPA structure resulting from the analysis.

Table 28 STPA result summary

Symbol	Name	Number
ACC	Accidents	6
HAZ	Hazards	6
CA	Control Actions	27
UCA	Unsafe Control Actions	119

Table 29 Examples of UCAs by type

Type: Given incorrectly
Performing inbound check without the correct experience is hazardous
Providing purchase order confirmation when the purchase order has been cancelled is hazardous
Providing the transport payment order to the wrong Transport Agent is hazardous
Providing transport payment order cancellation when there has been correct/complete product delivery, is hazardous
Providing transfer if funds for the incorrect amount is hazardous
Providing a service order activation when there has not been a purchase order confirmation, is hazardous
Providing service order cancellation when there has been a false Purchase Order Cancellation is hazardous
Type: Wrong timing
Providing Supplier Payment Order before there has been product validation is hazardous
Providing Product Validation before there has been a product and documentation reception is hazardous
Providing product reception before the correct supplier has been confirmed is hazardous
Providing purchase order confirmation before the product has been confirmed is hazardous
Providing transport payment order cancellation before the correct product delivery has been confirmed, is hazardous
Providing transfer of funds to supplier before the correct payment amount has been confirmed is hazardous
Type: Not given
Not providing Order Payment Confirmaton when there has been a supplier payment order is hazardous
Not providing Purchase Order Activation when there has been a confimed requirement is hazardous
Not performing inbound check when the product and documentation has been received is hazardous
Not providing transport payment order when there a product delivery confirmation is hazardous
Not providing transfer of funds to supplier when there has been confirmation of delivery is hazadous
Not providing transport documentation when the product pickup takes place is hazardous

5.3 Summary of the chapter

This chapter described the results of using the systemic risk analysis method STPA to the analysis of a series of cases of organizations exposed to cyber-attacks. It started by giving a description of the cases where this method was applied. The chapter ended by describing the results that were obtained from the STPA application.

Before analysing the answers to the research questions, it is first necessary to expand on the application of another method, for bridging one of the gaps found in the literature review, namely the static versus dynamic methods, i.e., the consideration of time in the resilience design for an organization. The next chapter describes the dynamic simulation is described,

Thereafter, in chapter 7, the results of both methods are used to answer the research questions.

6 Results: cyber-risk dynamic simulation

This chapter contains the result of applying the system dynamics simulation method to the case of a cyber-attack with operational consequences. The chapter starts by giving a background to the use of the method, to then give a background to the case upon which the simulation is based. The case is then described in detail. Thereafter the model is developed sequentially first its causal structure, then its hierarchical control structure to finally describe a resulting system dynamics model.

The dynamic simulation is developed as a proposal for answering the research question RSQ4.2 which was derived from the gap identified during the literature reviews concerning the importance of understanding the development over time of the response in supply chains to cyber-attacks, as a direct indicator of the resilience present in that supply chain.

This method is applied to a case of a company subject to Intellectual property theft. As a result, this chapter starts by providing background information in relation to the relevance of cyber-risks for the Intellectual Property (IP) management, to then proceed to describe the case upon which the dynamic simulation is based.

6.1 Cyber-risk on intellectual property

The complex digital networks that have resulted from the increasing use of IT in supply chain operations have created new sources of risk, related to 1) intrinsic programming flaws in these IT systems that make unintended user error more likely, 2) logic flaws in the connections between system components that result in failure risk even if all parts of the supply chain work as expected, and 3) external risks of unauthorized agents exploiting vulnerabilities and abusing these for their own benefit.

Intellectual property (IP) is an example of a particular organizational asset which has increased its exposure to theft through the use of IT for its transfer, storage, and development coordination. IP is defined as "*an idea, invention or process that derives from the work of the mind or intellect*" (Merriam-Webster, 2017). IP is thus differentiating knowledge that adds value to the organization that is aware of having it, and is considered as an intangible asset, whose unauthorized use might result in losses to the target organization. IP can takes the form of patents, copyrights, industrial design rights, breeding rights, trademarks, trade dress (for example the trademark Coca-Cola has over the shape of its bottles) or trade secrets for example.

The protection given by the state to an invention is a principle that was recognized as early as the fifteenth century, as it was in the City of Venice that that first patents were granted (Kanwar et

al., 2003), however the protection of this IP has been a matter of debate for at least the same amount of time. Those in favour of a weak protection argue for 1) the effect it would have on the markets due to lower prices and more competition as a result of widely available IP, 2) lower costs for the acquisition of technology, 3) the avoidance of patent abuse by publishing distorted patents to the detriment of those using the patent who are not the creators, and 4) the availability of technology for human advancement by avoiding "*sleeping patents*", i.e., patents that are purposely kept out of the market, strategy used by some to preserve market shares (Gilbert et al., 1982)

However, in the global context, IP protection has continue to spread. Since IP is a central driver for innovation, business growth and competitiveness (Bosworth, 2001; Bekkers et al., 2002), and a valuing process for IP has gradually increased, with current IP asset value levels potentially constituting as much as 80 percent of a single company's total value (Ocean Tomo 2015). As can be seen in Figure 65 the proportion of the Standard & Poor 500[29] index company values that corresponds to tangible versus

[29] The Standard and Poor Company in New York created an index in 1957 to track the value of 500 large companies, and is along with other indexes such as the NASDAQ or the Dow Jones, an indicator about industry composition and capitalization.

intangible assets, has changed dramatically. Intangible assets are partially composed by the IP in the company, and their share of the total company value has dramatically increased over the last 30 years: while in 1985 intangible assets were only 32% of the total value of the companies in the S&P 500, this has increased to 87% in 2015.

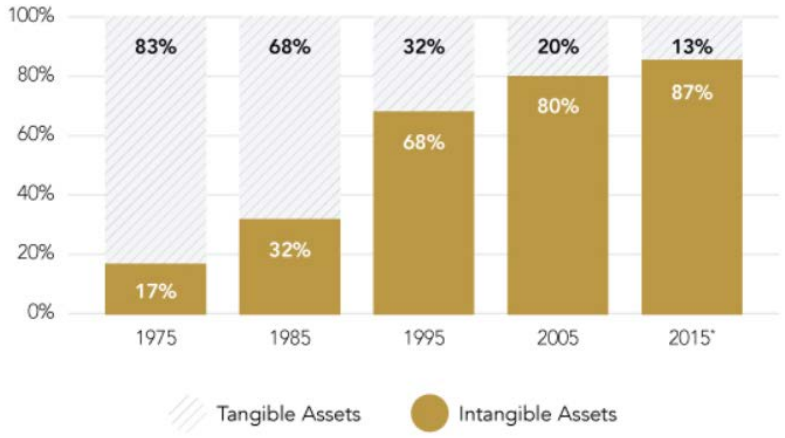

Figure 65 Components of S&P market value (Ocean Tomo, 2015)

This does not necessarily mean that all this value has been created in the company and only amounts to the valuation that has been given to that know-how in the company, to consider them assets in the formal accounts, and to manage them as such. For example, a company might have a process developed in-house, without having assigned it explicit value. Yet, when a decision is taken that this know-how is a differentiator in the market, it

becomes a piece of property that needs to be defined and protected.

Additionally the Sarbanes Oxley regulation, enforced after the Enron and Worldcom scandals, has imposed accounting rules that resulted in greater reporting detail requirements for IP valuation. This has transformed IP from being an internal strategic factor, to being a public financial dimension (Kossovsky et al., 2004). Literature informs that the most advanced economies are those with the greatest cyber-related IP losses, theft that accounted for as much of the US$ 200 billion cybercrime losses during 2013 (McAfee, 2014).

Traditionally, IP risk took the form of people inside the organization, with direct knowledge and access to Research and Development (R&D) resources, who misappropriated prototypes or documentation, physical or digital. This restricted the potential suspects in cases an IP theft took place, and it was usually an action targeted to specific documents or technology.

The digitalization of IP coordination and information transfer and storage, has opened the field to IP thieves in any location, allowing them to operate in relative anonymity. The pool of suspects is thus far greater, and can include competitors, hackers that do this for money or fun, or even nation-states. IP theft can in this case be either a targeted or opportunistic (Mossburg et al., 2016).

The way a company responds over in time to an event such as IP theft determines the extent of the consequences derived from this disruption. This has been called dynamic response or resilience. Sheffi and Rice (2005) showed the relevance of this dynamic response in supply chains through what they named a "disruption curve", which proposed representing the extent and depth of supply chain performance change as sources of economic loss during an unexpected disruption. Following such a framework, an improved response to disruption would consist of both a shorter and a shallower disruption in performance. This curve is seen in Figure 66.

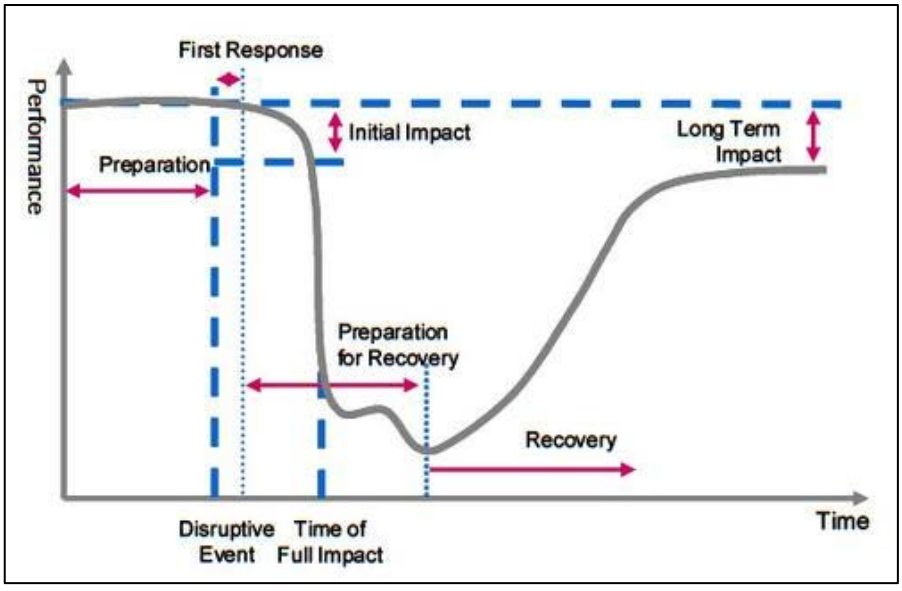

Figure 66 Disruption curve (Sheffi et al., 2005)

Sheffi& Rice were not the first to postulate a dynamic understanding of processes. Asbjornslett et al. (1999) proposed an

approach for assessing the vulnerability of production systems through the representation of the way in which a stable state is achieved by a disrupted system, as shown in Figure 67.

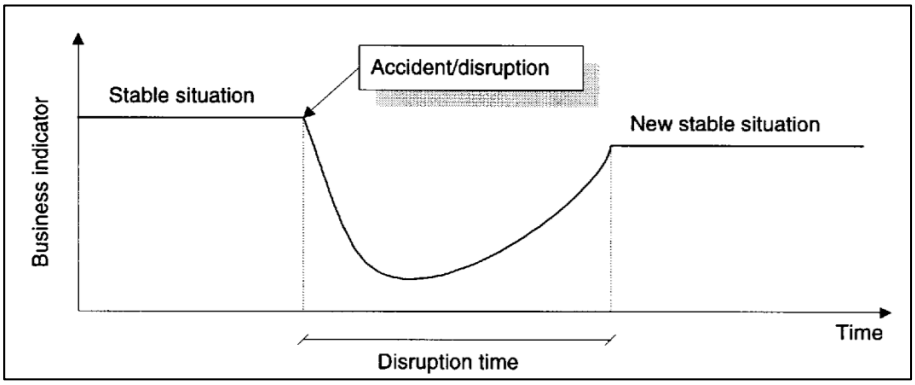

Figure 67 Stability regaining curve (Asbjornslett et al., 1999)

It can thus be said that Sheffi & Rice built on Asbjornslett et al. (1999) by identifying the different stages in the recovery process following a disruption, and by extending its application beyond productive processes to supply chains, and through the identification of resilience-building factors, despite not proposing any measures for resilience.

Tierney et al. (2007) proposed the resilience "triangle" as a way of quantifying the resilience of a system as seen in Figure 68. According to this approach, this triangle should be minimized shorter and shallower effects imply a higher resilience. No identification is given to the relative importance of shallowness and duration, but this seems to point to at least two dimensions in

the resilience response: how deep the effects are during a disruption, and how long these effects last.

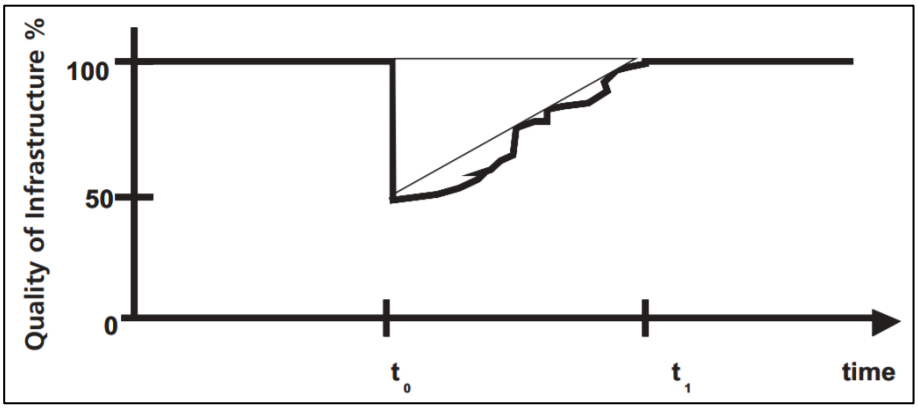

Figure 68 Resilience triangle (Tierney et al., 2007)

Furthermore, Zobel et al. (2014) have extended this concept of the disruption curve and the embedded resilience triangle to multiple disruptions, where subsequent disruptions happen before the system has regained a stable performance. This is shown in Figure 69.

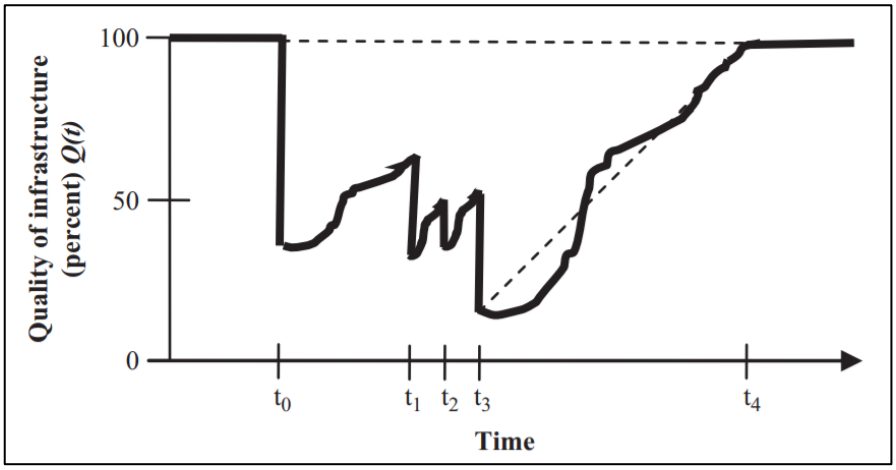

Figure 69 Multi-event resilience graph (Zobel et al., 2014)

6.2 Case description

ABC Industries is a US$ 40 billion producer of hardware for continuous connection to a communication network, also known as the Internet of Things (IoT) based in Silicon Valley, California. The internet of things has been identified as the inter-connection of physical devices, also known as smart-devices, including vehicles and buildings, by embedding them with elements such as sensors, actuators, electronics, software, and network connectivity, thus allowing these elements and devices to collect and exchange data.

ABC Industries, with 60.000 employees and a 12.2 percent operating margin had recently finished an investment in production facilities, resources for research and development (R&D) and marketing, aimed at the development and release of a core line of IoT network products. These products were based on proprietary technology in hardware production and materials, and in the software and information processing capabilities of the products offered to the market.

ABC Industries has a R&D department hierarchically dependent from operations management, shown in Figure 70.

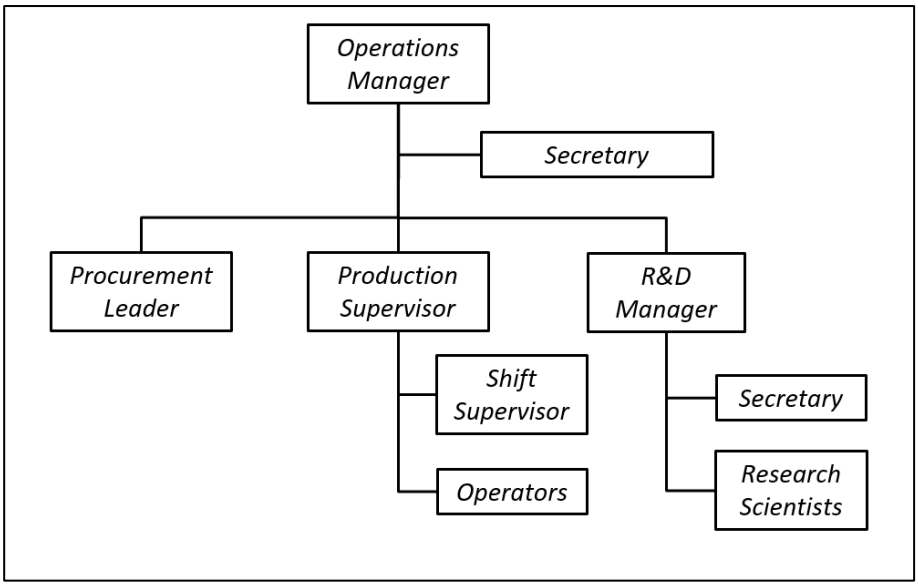

Figure 70 ABC Industries organigram

Six months before the product launch a federal agency informed ABC a cyber-breach at one of its facilities where the development of this line was taking place. Until that moment, ABC Industries had no indication of a breach or any consequences thereof.[30]

[30] This is one of the most recurring aspects of cyber-attacks and which differentiate these types of risks from other supply chain risks: a company may be under attack for much longer than it is aware of the attack. As long as operations are not disrupted, supply chains are unable to detect the breach as they have limited sensing capability. Additionally, information can be copied without any effect on the quality of the original information source, and a leak may be invisible to the organization from an operational point of view.

The initial assessment of the effect of this breach showed that 15 out of the 30 product lines under development had been affected and their IP data probably stolen. The affected lines were expected to contribute 25 percent of the company's total revenue for the next 5 years. No clear motivation was identified for the hacker attack.

An initial analysis showed that the information that was stolen would allow a hacker to uncover and exploit previously undiscovered design flaws and allow a hacker to implant malicious code into these product lines. The implications were confirmed 30 days later, when a Silicon Valley blogger released the news of the breach, and indicated that these products could be reverse-engineered and become an eventual competitor of ABC by both beating them to market with a similar product, and undercutting them on price.

ABC's reaction can be divided into three main sequential and slightly overlapping phases: Incident triage, Impact management and business recovery.

During the incident triage phase, ABC took specific steps to bring in the necessary resources to assess the initial damage and prepare the organization for potential consequences of this attack. These actions addressed four areas:

- First, as a request from the board, a team of managers and research scientists formed a task force to oversee the efforts

to minimize the effects of this attack. This diversion of resources to unforeseen activities had negative effect on the productivity of the R&D and sales team. This diversion of resources was triggered by the decision that the company was under attack (as identified by management after the formal notification by the state agency).

- Second, an external cyber-security company was hired to investigate the leak, and patch the system to future similar attacks. The choice to have an external company do this analysis and forensics was largely based on keeping the option of identifying an internal source for the leaks, option which is more difficult to investigate objectively with a local team.
- Third, a law firm was hired to lay out the potential legal ramifications of the breach.
- Fourth, a public relations (PR) firm was hired to start preparing the commercial ramifications of this breach.

During the impact management phase, ABC Industries makes tactical changes with short-term effects on the use of existing resources, and resulting in changes to existing processes. ABC Industries decided to accelerate the launch of the product lines by two months. This both created a need for additional research personnel and overstretched the capacities of existing research personnel, decreasing productivity. Additionally, product

shipments were suspended while an upgrade was developed for the products as a result of the stolen IP. Important contracts were lost probably as a result of both a decreased perception of product safety in the customers, and by the delayed shipment of existing orders. Contract losses were expected to account for 5 -10% of the projected revenues for the company.

During the recovery phase, ABC industries undertakes structural changes derived from the cyber-attack. First, it performed an inventory of all its IP, classified these, and instituted a protection program. ABC also upgraded its security infrastructure.

Figure 71 is a qualitative representation of the impact of the different actions taken by ABC Industries after the discovery of the incident.

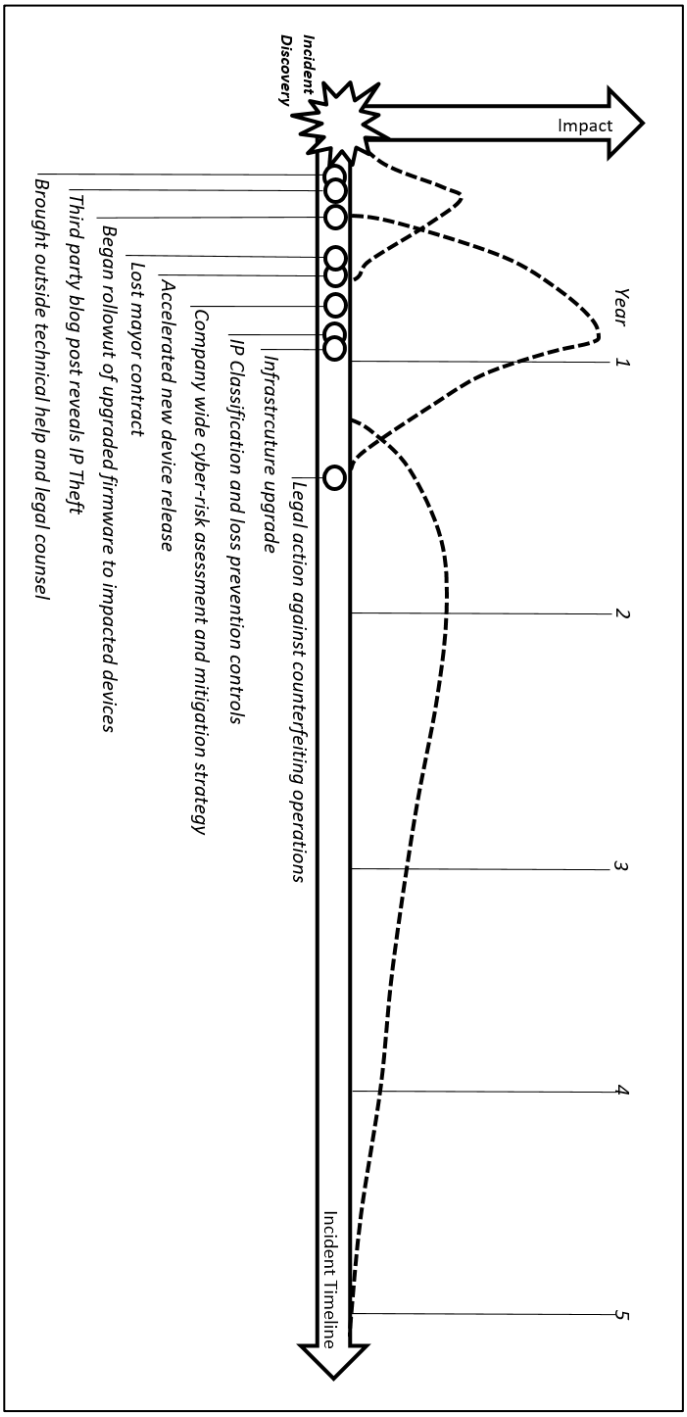

Figure 71 Timeline for disruption (based on Gelinne et al, 2016)

6.3 Reference mode underlying the problem

Overall, ABC industries reported this cyber-attack had additional costs of US$ 3.2 billion, and although their sales level returned to normal levels after one year, the total recovery time, indicated as the point when no additional costs were incurred because of the attack, was of five years.

ABC Industries reported the relative costs of their operations with respect to the expected cost of operations. This is:

$$Relative\ Value = \frac{Actual\ Value}{Expected\ Value} \qquad \textit{Equation 5}$$

The relative values were shared as in this way, they would able to provide the evolution of the financial effect of the attack without disclosing information which would be sensitive to their competitive position.

Figure 72 shows the evolution of the relative sales and profit levels with respect to the expected sales and profit levels. The complete data series can be found in the appendix 11.4. This is in essence the behaviour that is to be reproduced by the model, despite this not being the main aim of the model.

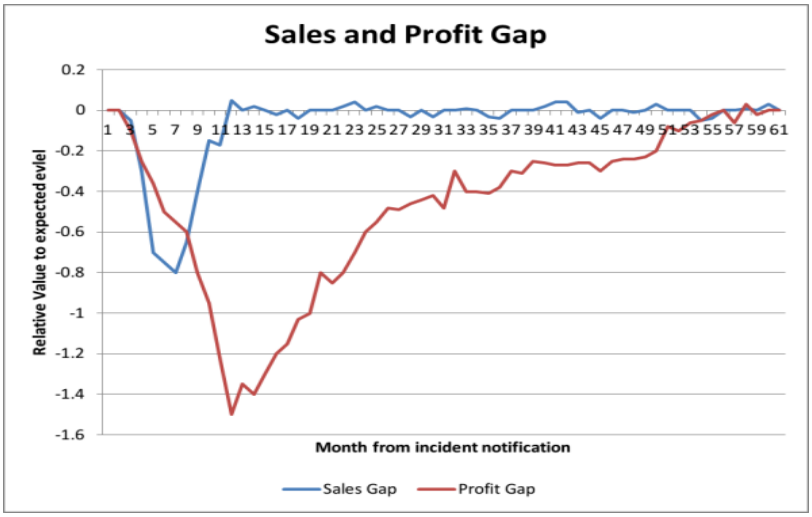

Figure 72 Sales and Profit Gap relative to expected values

6.4 Model development - causal description

From the case description, two ways through which ABC tracks the overall performance of the business were identified. The first is the Sales Gap, i.e., the difference between the Actual Sales and the Expected Sales. Operational measures are predictive indicators that determine the financial performance that is required. Although these are not the only possible performance measures (Hansen et al., 1989; Orlitzky et al., 2003; Prentice, 2016), this choice is consistent with what has been reported in literature as relevant financial performance indicators (Venkatraman et al., 1986), and it is what has been chosen as an initial performance target for this model.

From the interviews, the Actual Sales level is mentioned as being affected by the Demand, derived from the number of Base

Customers, and from the level of differentiation of the product, i.e., from the number of distinctive IP features it contains. From the description, the Sales Gap is relevant in the short term, as it is mentioned to have been recovered after 1 year of the attack having been detected.

The second performance measure is the Profit Gap, i.e., the difference between an actual and an Expected Profit level, Through the case description it can be derived that the Profit Gap is more relevant in the long term, as it is mentioned that although the Sales Gap was closed after one year, there were still additional costs in the company derived from the IP theft recovery, and which finally closed this gap after five years. In a general way, therefore, a series of circular causality feedback loop "types" can be identified.

- A first type corresponds to those feedback loops that form vicious circles with respect to the current performance levels. An example of this performance reduction is the loss of contracts derived from the IP theft. The more contracts or sales are lost, creates an even lower sales level increasing the sales gap and the profit gap.
- A second type of feedback loops, are those that the company uses to manage the short term actions, which have been denominated "*flexibility options*". These require either additional costs or a redistribution of existing resources, as

in the short term there has been limited time to increase the resources. As resources, the case mentions mainly management and R&D personnel. This second type can be in itself divided into two subtypes: either a redistribution of management resources at no additional cost, but with the effect of loss of productivity, and another is the hiring of external resources, available quickly, but at additional cost, such as the case of the Public relations firm, the cyber-security company and the Law firm that were hired. Both of these options have an effect on the performance, through a decrease in the IP generation efficiency, and through the increase in operation costs, respectively.

- A third type of feedback loops are those that the company uses to manage the long-term actions, which have been denominated the "*recovery options*". Examples of this include the additional Research and development personnel that was hired for the generation of additional IP. These have effects on costs and are the last ones to be maintained until the company reaches the expected operation level.

Figure 73 shows these generic feedback loop types.

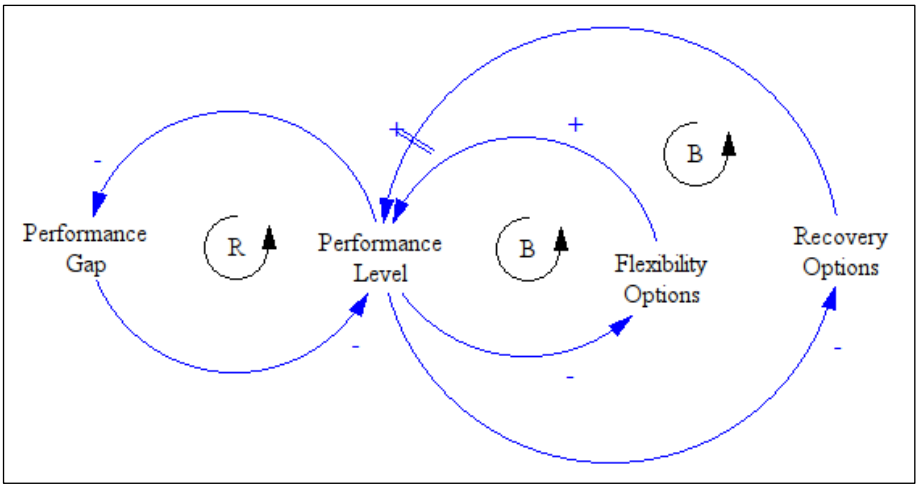

Figure 73 Main generic feedback loops during resilience

The data contained in the description presented in the previous sections can be converted into a series of feedback loops driving circular causality effects throughout the process. Consider the description example: "*…ABC hires a top public relations (PR) firm to reach out to stakeholders and create a face-saving public image campaign*". This description example contains at least two causal loops.

- On one side the PR firm is hired because of the decrease in sales and resulting increase in the deficit of the expected profit, due to the decrease in the number of customers derived from the IP theft. The hire of this PR firm should result in an increase in the customer base that should lead to an increase in sales. The individual polarities represent the dyadic relationships between the constructs or variables in the loop (e.g., an increase in sales results in a decrease in

the sales gap, being therefore a negative polarity). This is a balancing loop, as it is meant to regulate the variation in any of its constituent variables. For example, a decrease in sales, by going "*around the loop*", i.e., evaluating each of the dyadic relationship polarities in sequence, results in an increase in sales, thus regulating its value.

- A second loop included in this description considers the circular causality resulting from the increase in costs due to hiring this PR firm, which leads to an increase in the expected profit deficit, which results in even more required activity. This is a reinforcing loop, since if it was the only feedback loop present, would lead to a permanent variation in any of its constituent variables and constructs.

The following table contains a list of the feedback loops identified in the description, which are explained in detail next.

Table 30 List of feedback loops contained in the case description

Loop Number	Loop Type	Loop Name	Loop Number
1	Reinforcing	R1	IP Rules
2	Reinforcing	R2	PR to the rescue
1	Balancing	B1	Marketing Stabilizer
2	Balancing	B2	IP Expiration
3	Balancing	B3	Marketing Costs
4	Balancing	B4	Hacker Attacks
5	Balancing	B5	Trust issues
6	Balancing	B6	Productivoty Loss
7	Balancing	B7	Security Costs
8	Balancing	B8	Legal Bundle
9	Balancing	B9	Legal cousel
10	Balancing	B10	Legal costs
11	Balancing	B11	PR Costs
12	Balancing	B12	Leak containment

In order to facilitate the presentation of a complex causal loop diagram, this is shown sequentially in the following stages:

- *Stage 1*: Base diagram: represents the loops involved in the company as a business based on the development of unique Intellectual property.
- *Stage 2*: Incident Management diagram: represents the base diagram plus the loops involved in the short-term reactions of ABC Industries, particularly the Triage and Incident Management reaction phases. As such, it integrates external resources and the resulting costs, as well as the reallocation of existing resources with the subsequent effect on productivity.

This logic is maintained when developing the stock and flow diagram. The base diagram is shown in Figure 74. The main Feedback loops considered in the dynamic of the base company are:

- *R1, reinforcing loop 1, "IP Rules" feedback loop*. This loop captures in a general way the main mechanism through which a company based in exclusive IP develops its business. Exclusive IP generates a Demand which is translated into Actual Sales and Actual Profit levels, which are partially invested into the development of more Exclusive IP, expanding the business
- *B1, balancing loop 1, "Marketing stabilizer" feedback loop*. This loop captures the main mechanism ABC Industries uses to counteract differences in demand. Since the development of IP is a long, uncertain process, which is then reflected as exclusive products to the market, the way in which demand fluctuations are counteracted are through changes in the sales strategy using the same existing resources, and through the use of marketing instruments such as promotions. This creates a loop that eventually does not let the Sales Gap to increase endlessly.
- *B2, balancing loop 2, "IP expiration" feedback loop*. This loop captures the process of IP expiration, resulting from the limited time for which an IP is exclusive to the company

that created it. For technological developments this expiration period varies from 15 to 25 years. This is a balancing loop which if existing on its own, would result in the company not having any Exclusive IP after some time, generating the need for continuous IP development to maintain the Exclusive IP difference which is responsible for the demand.

- *B3, balancing loop 3, "Marketing Costs" feedback loop*. This loop captures the important fact that the marketing which allows the company to recover demand, also leads to additional costs, limiting the amount of marketing that can be done, as it affects the profit level with a direct consequence in the number of R&D projects that can be started.

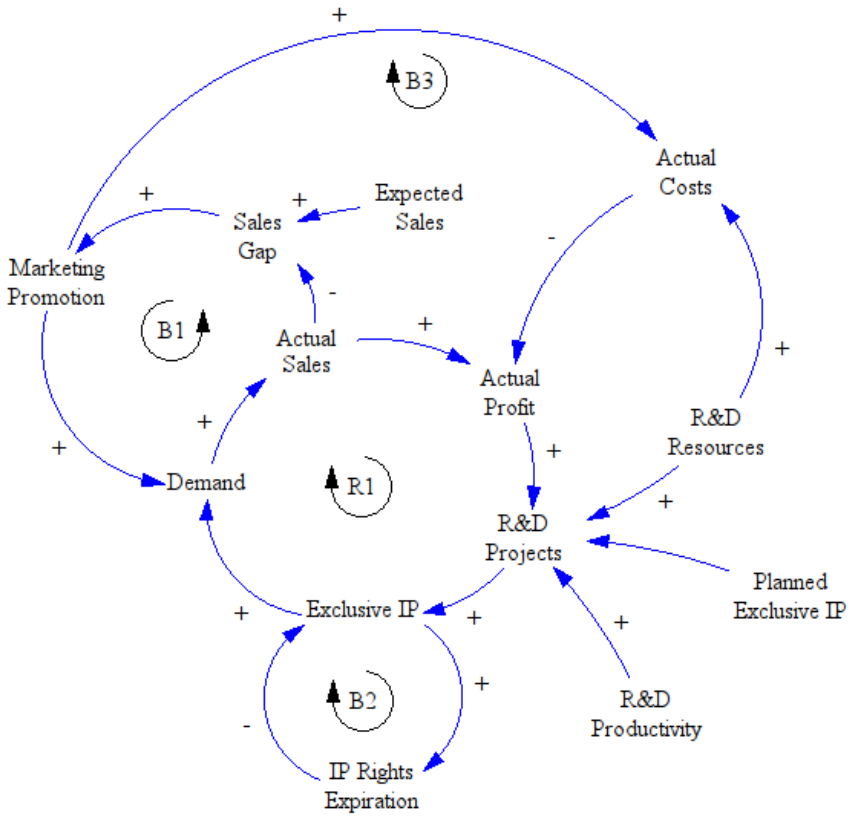

Figure 74 Causal Loop Diagram - Base Diagram

The model diagram for stage 2 included the actions for incident management, reflected in the following Feedback Loops:

- *B4, balancing loop 4, the "Hacker Attacks" feedback loop*, which captures the effect of the attractiveness of exclusive IP to external agents who attempt to steal them. This, all else equal, creates a balancing loop limiting the number of exclusive IP a company can attempt to have.
- *B5, balancing loop 5, "Trust issue" feedback loop*. This captures the effect that a hacker attack has on the trust of

the product by the customer base, through aspects such as resulting product safety. By stealing IP, hackers have access to the technology, and this enables them to identify design flaws or introduce viruses into the resulting products. The lower Product Safety that results from Hacker Attacks affects the base customers through effects such as loss of contracts or a lower level of general sales, as indicated in the case description.

- *B6, balancing loop 6, the "Rearranging Productivity" feedback loop*. This loop accounts for the short term effects of reassigning existing company resources to managing the incident, both during the triage and incident management phases of the case description. As the case mentions the short-term reassignment of resources, R&D and management personnel derived from the decision to accelerate the product line launch by two months, results in lower productivity which stretches beyond the short term and well into the long term recovery. As a first approximation, is represented as in direct result of the organizational pressure to manage incident.
- *B7, balancing loop 7, the "Security costs" feedback loop.* This loop accounts for the economic effects of engaging a cyber-security company to identify and eliminate the IP leak (effect contained in Loop B12). These services create additional costs which reduce available profit.

- *B8, balancing loop 8, the "Legal Bundle" feedback loop*. This loop represents the generic effects of a hacker attack in the legal realm, one of the first areas ABC Industries set out to manage once the hacker attack was declared. The loop captures the higher incidence of lawsuits from the hacker attack, and the loss of customer base and sales as a result.
- *B9, balancing loop 9, the "Legal Counsel" feedback loop*. This loop captures one of the measures derived from the pressure to react to the attack, which was to hire a legal firm. This hire has an effect on the number of hacker-attack-related lawsuits, limiting their negative effect on the organization.
- *B10, balancing loop 10, the "Legal Costs" feedback loop*. This loop reflects the costs associated with the hiring of the legal services, with an effect on overall organizational Actual Costs, and reduced Actual Profit.
- *B11, balancing loop 11, the "PR Costs" feedback loop*. This loop captures the costs of hiring a PR firm, one of the first actions undertaken by ABC Industries once the hacker attack was declared.
- *B12, balancing loop 12, the "Leak Containment" feedback loop*. This loop reflects the result of the initial measure undertaken by ABC industries once the hacker attack was declared of hiring a cyber-security company to detect and

contain the data leak. This action results from the organizational Pressure to Manage the Incident, which results in the securing of IP.

- *R2, reinforcing loop 2, the "PR to the rescue" feedback loop*. This reflects the virtuous cycle resulting from hiring a Public Relations company. The investment in this service should have a positive effect on the Customer Base that has an effect on Actual Sales level.

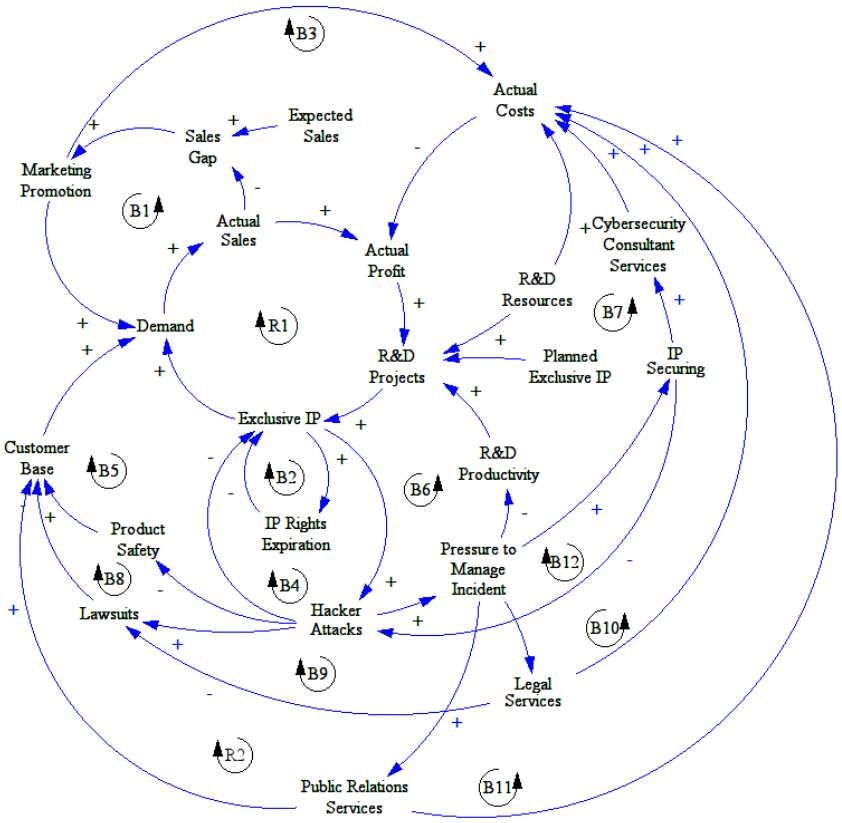

Figure 75 Causal loop diagram model with reaction

These feedback loops therefore represent a “translation” from the information gathered through documentation and interviews, into a causal loop structure to single out variables of interest, the relationships between these variables and the type of relationship (positive or negative polarity), and the circular causality structures and type (reinforcing or balancing loops) that are formed between these variables.

This creates an explicit representation of a common mental map that was contained in the documents and people from where the information about the system was obtained. However, this is still not directly associated with the formal structure of the system, and it is relevant to keep this relationship in mind when building a model that exists within a formal organization for at least the following reasons:

- A formal organizational structure associated to the causal structures that have been identified in this stage are *sometimes easier to communicate* to audiences that do not have a lot of experience in systems representation or systems design,
- When the behaviours are explained, it is *insightful to relate this to the different areas of the organization*, particularly if the research question that gives rise to this simulation is kept in mind: by identifying areas, compartmentalization

can be visualized and its usefulness or the difficulties created by it can be extracted.

- By relating the causal structures to the formal organizational structure, the *relationships that need to be contained in the model can be checked and updated*, particularly of all the input and outputs that exist in the normal operation are in fact contained in the model.
- By relating the causal structures to the formal organizational structure of the system, the *adequate level of aggregation can be better identified*, to see if a more granular or a more general analysis is necessary.

It is for these reasons, that the next section of this work describes the development of a hierarchical control structure, a mid-way step towards developing the dynamic model.

6.5 Model development - hierarchical control structure

The hierarchical control structure (HCS) as was shown in chapter 5, is a traditional tool used in engineering for the representation of complex systems to depict system composition, hierarchy of control and information flow. A HCS is proposed for the process of modelling of social systems due to a number of beneficial characteristics:

- HCS is a way of representing the different information flows present in the case study. Examples of information

flows in the case study include Resources Cost, Actual Sales, Stock of IP, Demand Level or Sales Level, for example.

- HCS is a way of representing the different instances where information is modified, in places denominated as "controllers". Controllers can be determined by identifying where information is transformed. For example, at some point the company, the Actual Sales, and Actual Cost is "transformed" into the Profit level, calculated as the difference between Sales and Costs. This controller has been denominated "Finance". Also, at some point, the organization transforms a required resource level into an actual resource level available in the organization. This is not represented as easily as a subtraction, but is a process that takes place in the "R&D Resource Management" area of the company.
- HCS as a way of controlling for required flows in the organization. Controllers can be represented and analysed individually, such as in Figure X. An analysis for each controller can help a developer identify required inputs
- HCS is a way of identifying and representing controller hierarchies, by positioning controllers in different horizontal levels in the diagram.

The process of creating a hierarchical control structure as a process of building a system dynamics model is not mentioned by all authors. Particularly Morecroft (2015) who proposes the "*sector maps*" approach to "*show the main interlocking subsystems or functional areas in which feedback loops are to be found, to convey a clear impression of the model boundary, and the assumed level of aggregation*" (Morecroft, 2015, p.140).

Beyond what Morecroft proposes as sector maps, this work has added a hierarchical representation of these sectors to develop what has been termed here a "hierarchical control structure", in a similar way as it was done for the case of the systemic risk analysis, the areas of the organization and the flows between them are identified. From the organizational data, the following sectors were identified:

- Corporate,
- Financial Management,
- Sales Management,
- Public Relations
- IP Management
- Resource Scheduling
- R&D Resource Management
- Performance Tracker
- Hacker
- Customer Base

When the inputs and outputs to each of these sectors are considered, then the following sector diagrams were generated. Each diagram shows the sectors that are directly related, as well as the information flows.

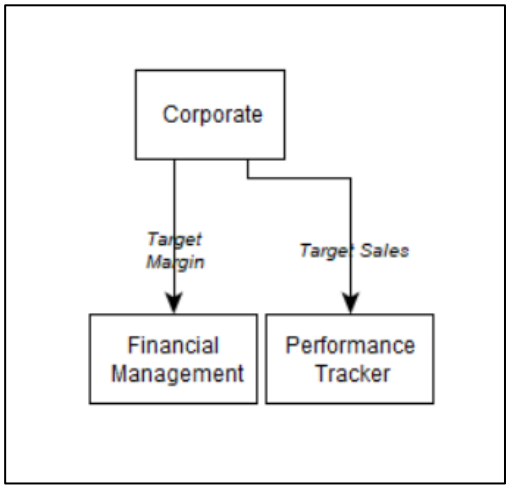

Figure 76 Corporate sector diagram

For the case of the corporate sector, it is considered as an exogenous variable, since it only generates outputs, this is the expected sales and margin levels, which are communicated to the performance tracker and financial management divisions of the system. This is not to say that Corporate does not have inputs, as these are also dependent on both the level of aggregation chosen for the model, as well as the boundaries of the system. In the case that the system had been considered of a broader scope, the inputs to corporate could have been stakeholder expectations, such as "*stockholder profit level expectations*", or market benchmarks, such as "*average margin for the industry*".

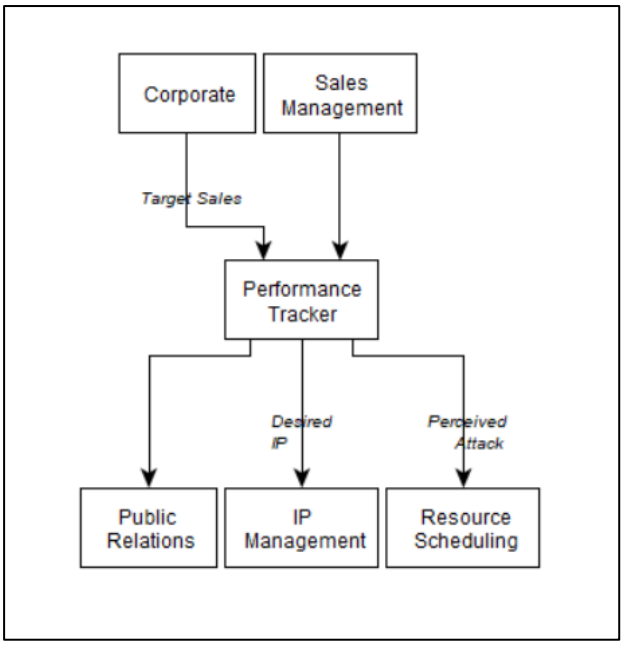

Figure 77 Performance tracker sector diagram

The performance tracker, as shown in Figure 77 is said to be an endogenous sector for the model, as it is dependent on inputs from the system. This performance tracker delivers important signals to the system, as it "*converts*" the inputs it receives, in this case "*Sales*" and "*Sales Target*" to the desired IP levels and the signal of attack perception. This las concept was indicated by some interviews as "*a recognition that an attack was underway*". For the case used in this simulation, the attack signal was external, triggered by the federal agency that informed the company of a cyber-attack taking place. These endogenous nature of the sectors is a common characteristic of the other sectors shown in Figure 78 through Figure 84.

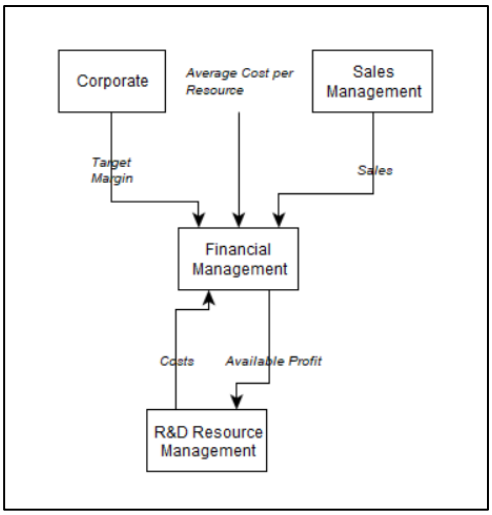

Figure 78 Financial management sector diagram

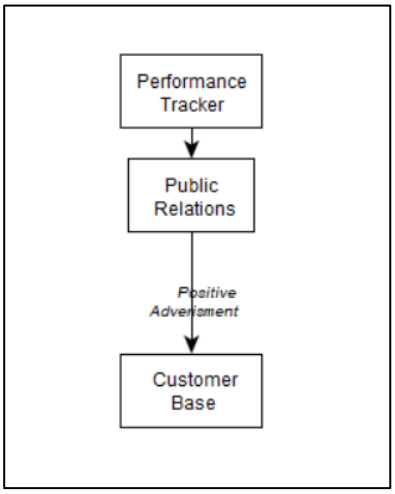

Figure 79 Public relations sector diagram

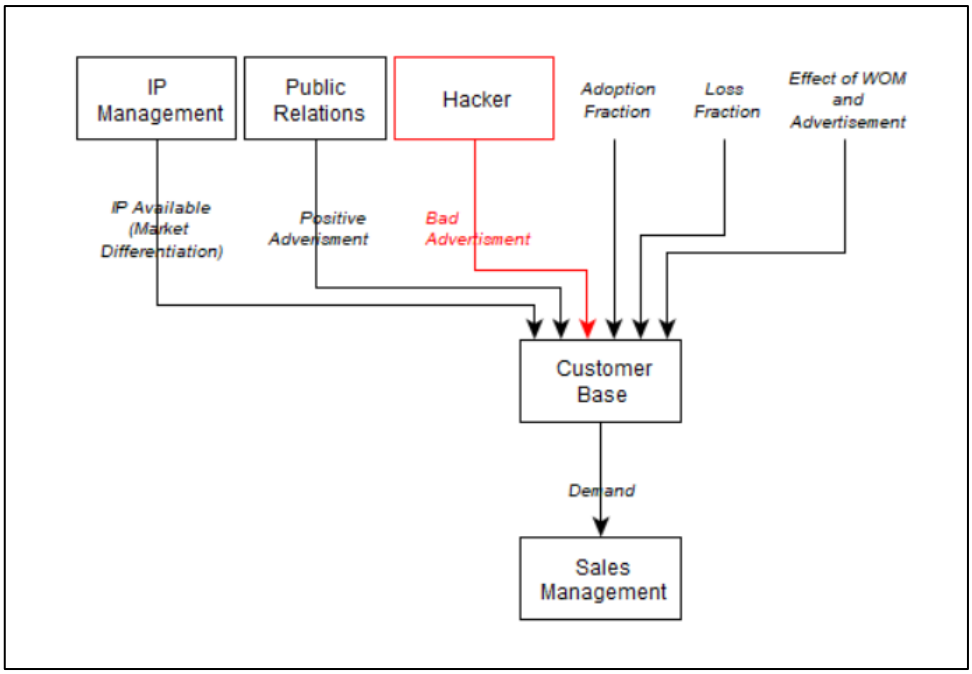

Figure 80 Customer base sector diagram

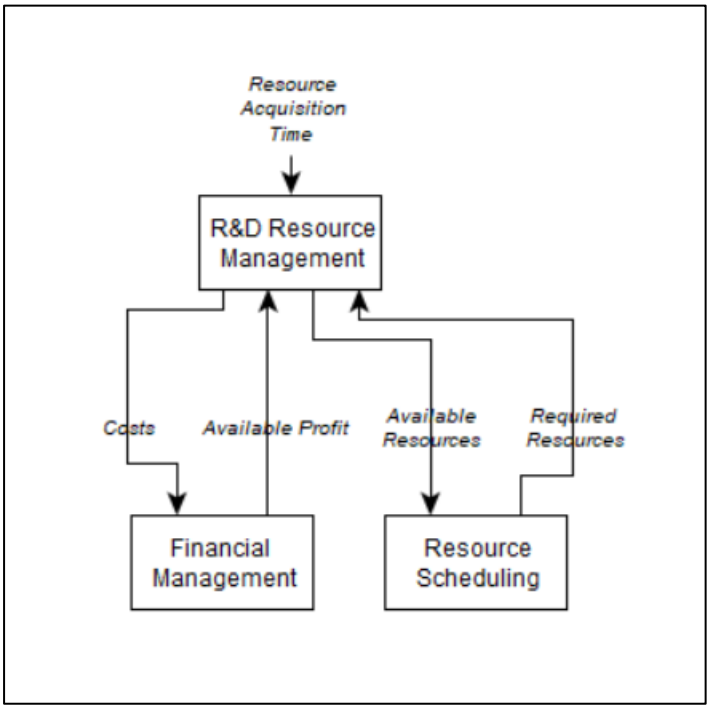

Figure 81 R&D Resource Management sector

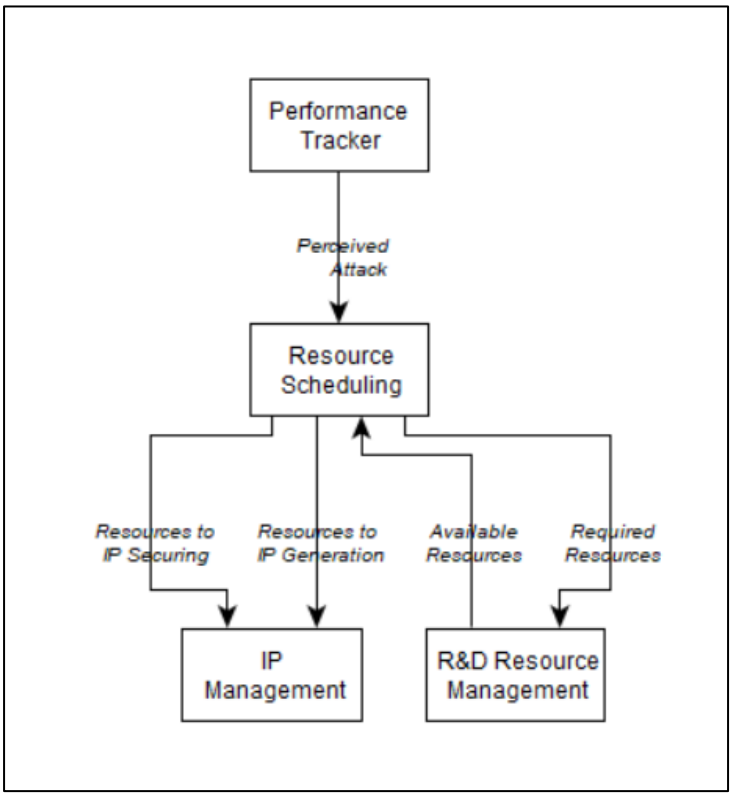

Figure 82 Resource scheduling sector diagram

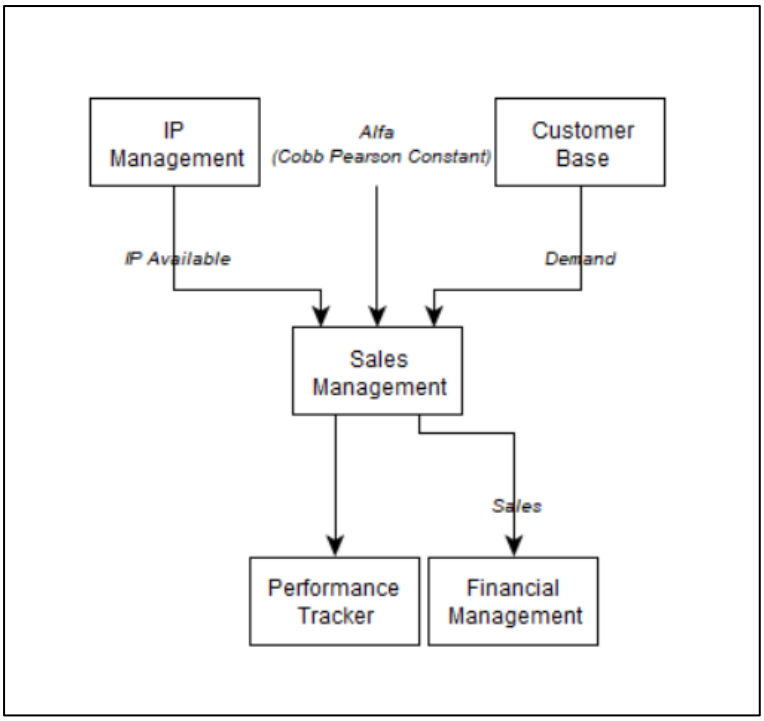

Figure 83 Sales management sector diagram

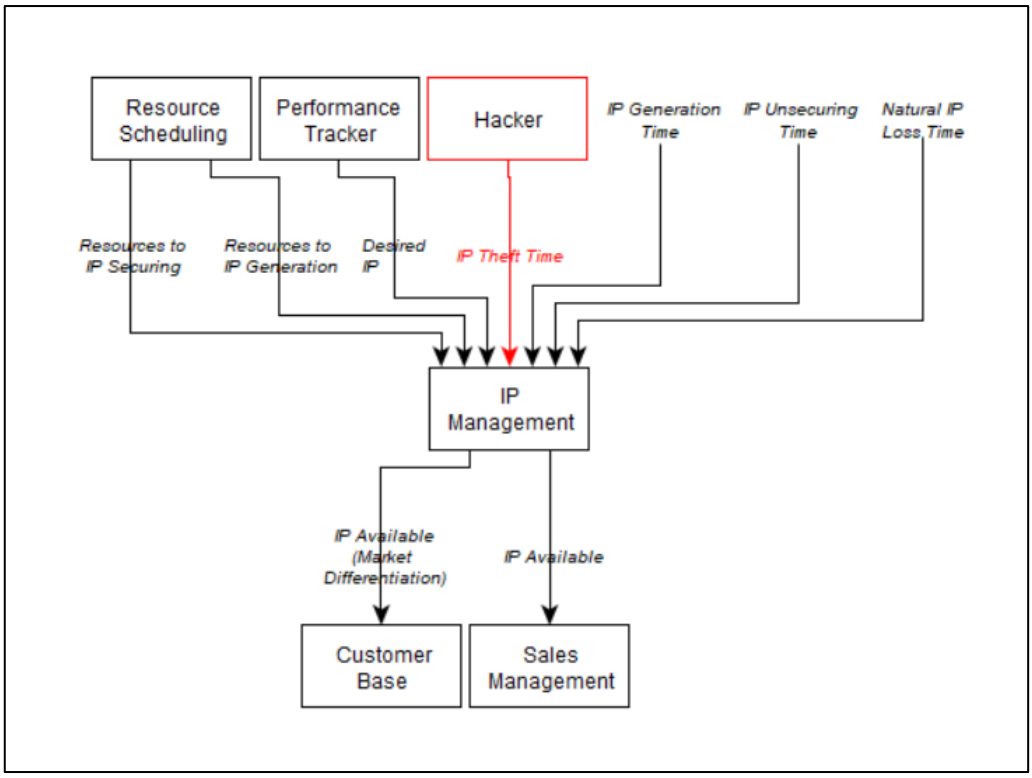

Figure 84 IP Management sector diagram

The last sector being represented, the "Hacker" sector is not a sector of the system, but it is an exogenous sector, but rather like Corporate, in that it influences the system with its outputs. The ways in which this model has considered the Hacker sector can influence the system is threefold, according to the description of the case:

- First, the Hacker sector can influence the loss of IP, the most evident of the effects, and which in the current case was communicated to the company by an external federal

agency. The way in which this loss is represented, is discussed during the development of the dynamic model.

- Second, the Hacker sector can affect the customer base, through some sort of "*bad advertising*" resulting from the confirmation of IP theft, particularly through public channels such as the blog posting. This effect is reflected in the case description through events such as the loss of important contracts sometime after the attack is made known.
- Third, the Hacker sector can affect the IP generation time, or the average time in which ABC industries can compensate for the lost IP. This is a way of reflecting the case description that indicates that the technical information was made public, and thus it was available for any other competitor to use without restrictions.

  These influences by the Hacker sector to the model, are shown in Figure 85.

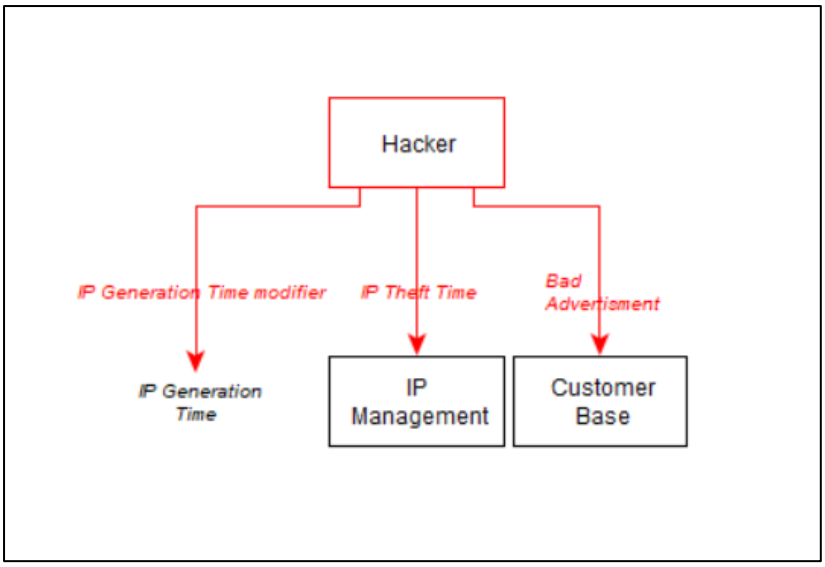

Figure 85 Hacker sector diagram

These are not the only ways in which a hacker can affect operations, but they are examples of more generic ways in which hackers can indeed affect operations. The generic types are the operational effects (i.e., effect on IP generation time), environmental effects (i.e., effect on the customer base), and resource-related effects (i.e., availability of exclusive IP). Examples of other options are laid out in the discussion section of this thesis.

The interaction between sectors can also be understood as representing three distinct levels of aggregation. The lowest aggregation is operational, an overarching aggregation to it is the strategic one, and finally the environmental aggregation level, which considers conditions external to the system boundaries that were chosen.

The overall HCS diagram integrates all these components: sectors, information flows and aggregation. Additionally, in the same way as in the hierarchical control diagram shown in Chapter 5, the hierarchy is considered in the final representation: sectors with more control placed higher up in the diagram. Figure 86 is a representation of this integrated HCS, showing aggregation in a concentric way, hierarchy in a vertical way, sectors as squares or nodes, and information flows as arrows. This representation allows for the straightforward identification of exogenous sectors (i.e., no arrow are going into them), some of the model assumptions (external variables going into a sector), how different levels of aggregation actually interact (e.g., information from Corporate going into the Operational level), and through the use of software such as yED (https://www.yworks.com/products/yed) the sectors can be quickly singled out and inconsistencies found out.

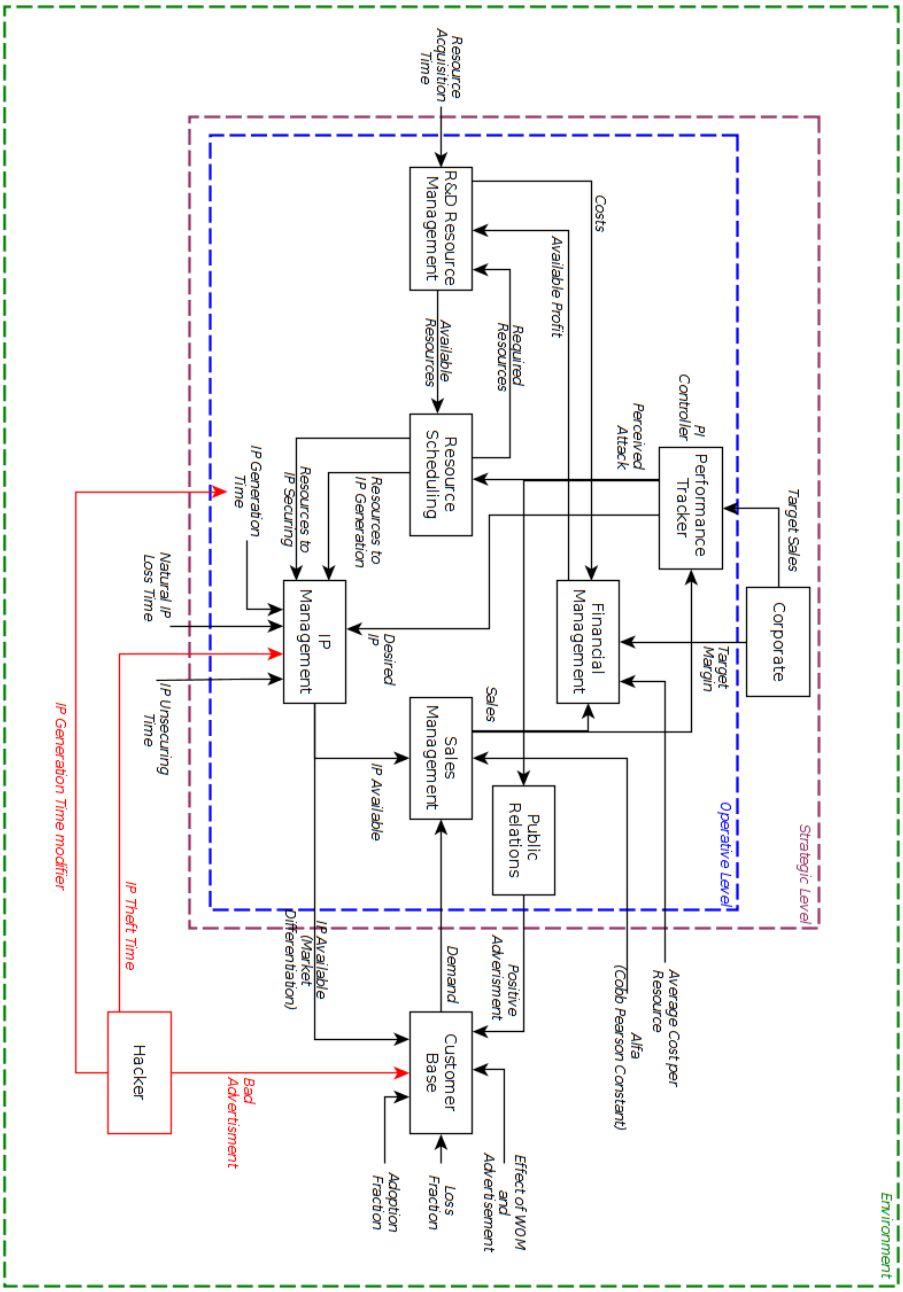

Figure 86 Hierarchical control structure

The HCS is shown in this work as an intermediate result in the process of building a stock and flow diagram, as it provides a good way of checking the different components in this system with respect to the inputs and outputs of each, and for identifying at a high level the variables that might be needed for the next step, which is to simulate the sectors in a dynamic model.

As a result of a HCS, it is now possible to build a system dynamics model by developing the sectors sequentially to then connect them. As it was indicated during the description of the method of system dynamics, it is highly recommended that a system dynamics model be developed in some kind of sequential way, to continually test and improve in an iterative process that culminates when the objectives of the model building process have been reached. This sequential building process is shown next.

6.6 Model development – stock-and-flow model

Starting from the causal loop diagram and the hierarchical control structure diagram, a stock-and-flow model was built in sequential stages, as was indicated in the section of this paper where the causal loop diagram development was mentioned, covering first the base model, then a model with the short term actions, and then a model including the long term actions.

The base model, based on the base causal loop diagram is shown in Figure 87. The equations for this model are detailed in appendix 11.5.

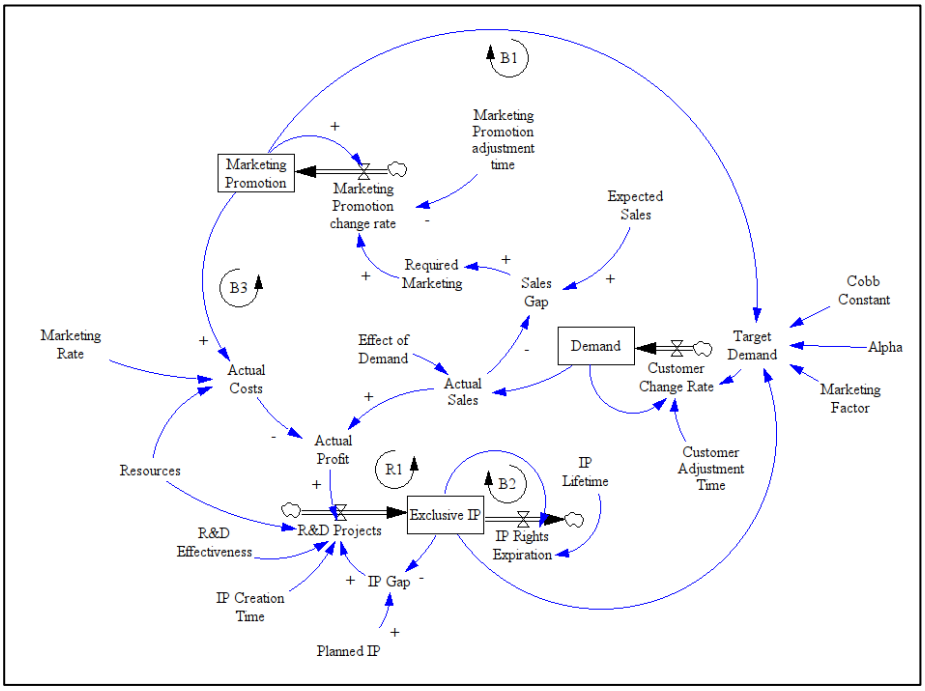

Figure 87 Base stock-and-flow diagram

The basic Reinforcing loop and balancing loops are indicated here in correspondence to the Base model contained in the causal loop diagram. The following aspects have to be noted:

- Three Stocks have been added to represent relevant delays in the base model. These are the stock of Exclusive IP, the stock of Demand (equivalent to the number of customers) and the marketing promotion, as these are an indication of the current state of the system.

- Relevant delays were not necessarily indicated in the Causal Loop Diagram, but became evident in the process of creating the stock and flow diagram. These have been indicated as the additional stocks mentioned in the previous point. These delays reflect the basic adjustments present in the system, and a first order information delay has been chosen as a way of representing these.

This first approximation for the model delivers a behaviour that is explored in section 7.3.

In order to explore more in detail the structure of an IP theft, an initial model can be described in terms of the interaction of four main areas 1) the inventory of intangible assets in the company, in this case the IP 2) the performance tracking, 3) the inventory of Resources, and 4) the customer base and the organizational resources, as shown in the stock and flow diagram in Figure 88. These areas have an equivalent in the hierarchical control structure diagram in Figure 86.

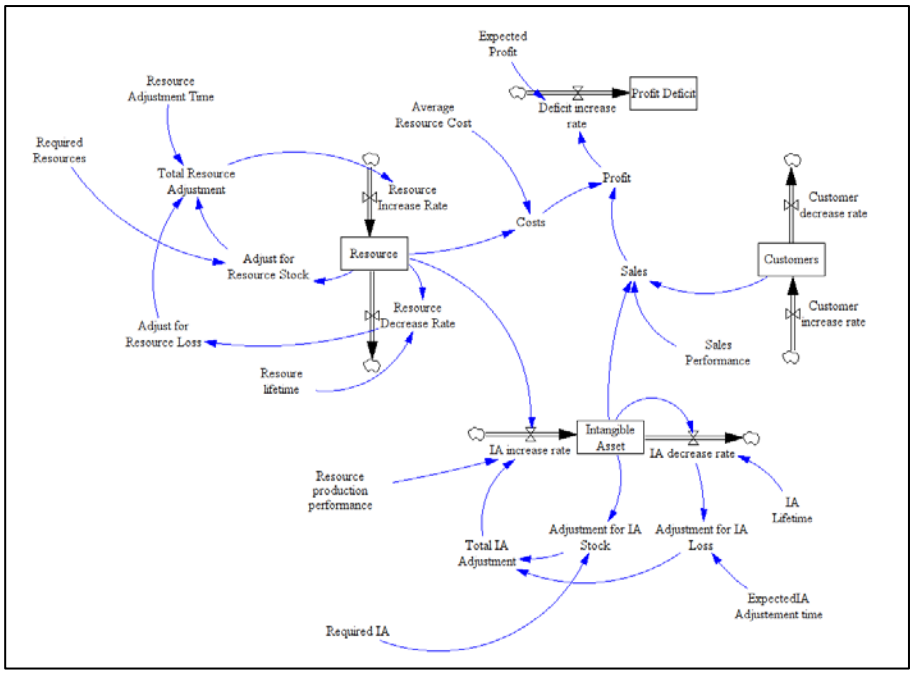

Figure 88 Basic areas interacting in the model

In order to build this model sequentially, and in order to focus on the aspect of the model that is most relevant to the problem, the Intangible asset area is developed in detail.

To reflect the process of securing IP once a cyber-breach is detected, a configuration was chosen that contains two stocks, one which represents the IP that secure, and another stock to represent the IP that is open to be hacked.. A division of the Exclusive IP stock into safe and unsafe stock is shown in the next figure.

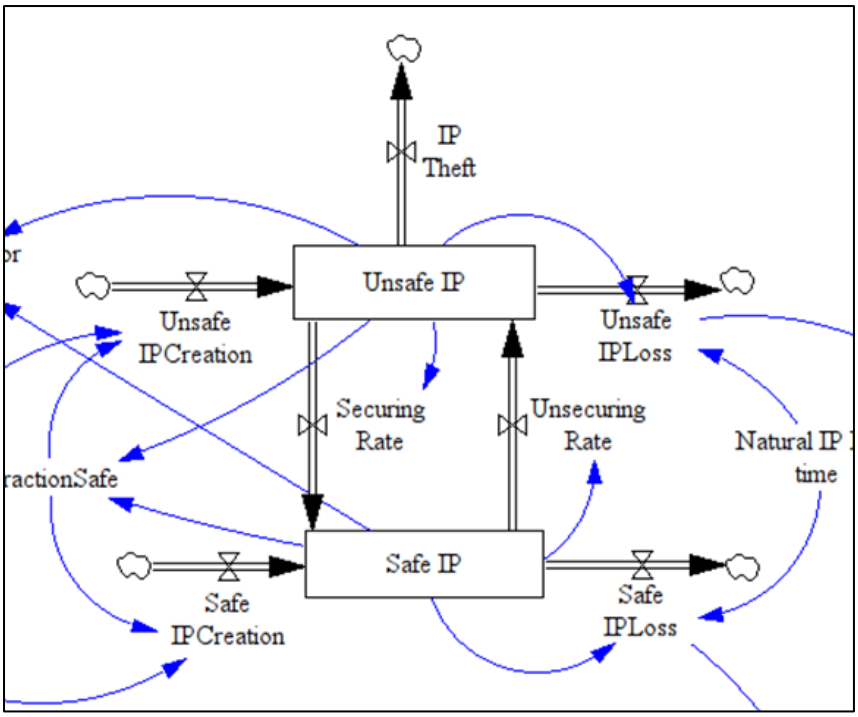

Figure 89 Advanced model detail safe versus unsafe IP

This double stock system represents the "physics" involved in the securing and un-securing of IP. The following must be noted:

- The IP theft can thus occur only from the unsafe IP.
- The "un-securing rate" is not zero, as IP becomes unsafe naturally if nothing is done to secure it.

Figure 90 shows this IP management "*module*" interacting with the performance management section of the model.

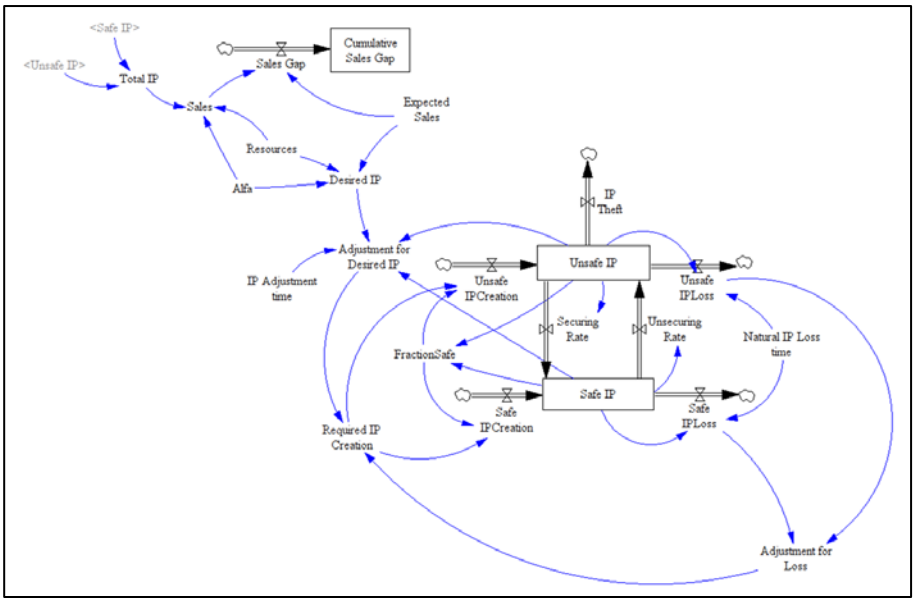

Figure 90 IP Management plus performance management

6.7 Chapter summary

This chapter described the result of applying the system dynamics simulation method to the case of a cyber-attack with operational consequences. The chapter gave a background to the use of the method, to then the chapter described background information to the case upon which the simulation is based. The case was then described in detail. Thereafter the model development was shown sequentially, first its causal structure, then its hierarchical control structure to finally describe a first approximation to its system dynamics model.

7 Discussion

This chapter presents an analysis of the results described in chapters 4, 5 and 6. Thereafter the research questions are answered from these results and implications to industry and academia are described. The chapter ends by outlining the limitations of the tools used in this thesis.

7.1 Analysis of the nature of cyber risks

This section will review the results for each of the research processes followed in this thesis, with a focus in the gathering of evidence to answer the research questions. First the analysis is presented for each of the processes, and then these analyses are combined as necessary to answer the research questions in section 7.4.

This section discusses the patterns and categories found in the cyber-risks from the cases gathered and presented in chapter 4, 1) by comparing cyber-risk groups between each other, and 2) by comparing the cyber-risk groups with other supply chain risks, according the method outlined in section 3.7.

7.1.1 Comparison of the different cyber-risks groups

The cyber-attack groups that are presented in Chapter 4, are grouped according to similarities in the structure that causes the operational disruption originating from the cyber-attack. Five groups were identified, namely 1) active theft of assets, 2) passive

theft of assets, 3) active product theft, 4) active interruption of operations, and 5) passive interruption of operations.

When comparing these five groups, differences are identified with respect to 1) hacker protagonism, 2) targeted versus non targeted approach, and 3) supply chain influence direction.

The *hacker protagonism* is related to the active versus passive role taken by the hacker to cause the disruption. An “active” cases group is defined as those groups of similar cases of cyber-attacks where the control action (see section 3.8.2) that leads to the operational disruption on the supply chain is executed by the hacker. On the other hand, a “passive” cases group is defined as the group of similar cyber-attacks where the control action that leads to the operational disruption is executed by the target organization as a result of a hack.

If these actions are caused by the hacker, then restricting the capacity of a hacker to execute these actions would address the problem. For example consider Figure 46 for the case of Tesco Bank. The disruption actions of using the credit card data to impersonate the customer in the purchase of resources, or in the case of Thyssen-Krupp (see Figure 48) the use of the stolen IP to create differentiated products or services, is a specific action on the supply chain, i.e., the supplier, undertaken by the hackers to crate the disruption.

However, in the case of the passive theft of resources in Leoni AG (see Figure 50), the email supplanting the CEO sent to the CFO does not affect the supply chain directly, but it is the CFO's instruction that results in the Bank sending resources to the hackers as a result of the disruption.

Comparison of the cases also reveals *targeted versus non-targeted* cyber-attacks, closely related to the active/passive categorization. Active sources require case-by-case actions by the hackers, posing a limit to the number of actions hackers can perform at any one time. For example, the active interruption to operations for the Bowman Dam or to the steel mill requires the knowledge of specific characteristics to each operation, as the controllers and equipment will vary between different organizations even within the same industry.

On the other hand a passive ransomware attack, for example, can affect different industries and geographies simultaneously. In the case of the Wannacry ransomware, estimates indicate that it affected between 150.000 and 200.000 computers in 150 countries, as can be seen in Figure 91 (Chappell et al., 2017).

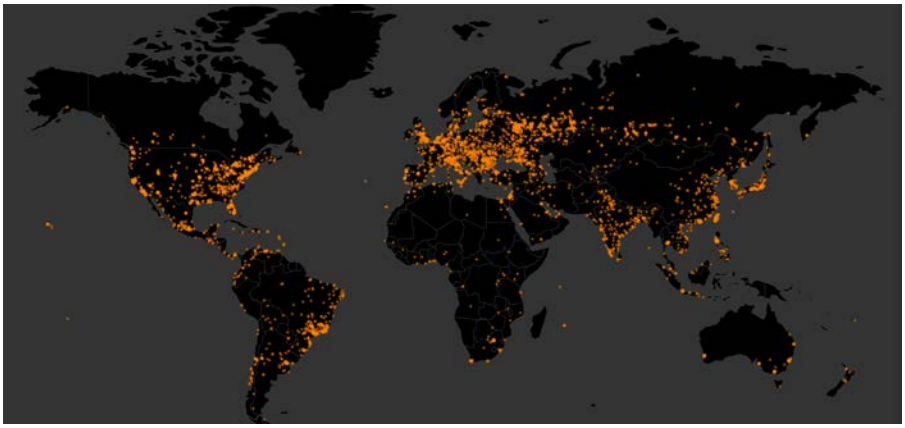

Figure 91 Wannacry attacks – one dot per affected computer

The cases in the gathered data also affected the *supply chain in different ways*. In the case of the active, targeted attacks the disruption is detected by the upstream supply chain, e.g., the customer in case of Tesco Bank losing funds, the Kia and Hyundai car being stolen from customers, or the nuclear plant or steel mill outputs being affected by disrupted operations. On the other hand, the passive, non-targeted attacks have disruptions felt by the downstream supply chain, such as Leoni AG suppliers not receiving payment, or the NHS service providers (Ambulances) having their operations disrupted.

These differences are summarized in Table 31.

Table 31 Comparison of cyber-risk sources

Operational disruption group	Disruption type	Hacker protagonism	Approach	SC influence
Group 1	Theft of assets/resources	Active	Targeted	Downstream
Group 2	Theft of assets/resources	Passive	Non-targeted	Upstream
Group 3	Theft of Product	Active	Targeted	Downstream
Group 4	Interruption of operations	Active	Targeted	Downstream
Group 5	Interruption of operations	Passive	Non-targeted	Upstream

7.1.2 Cyber-risks vs. other supply chain risks

The cases that are identified in the archival research are compared to other supply chain risks. The supply chain risks that are used for this comparison are identified in section 3.7.3 of this thesis:

- *Non-cyber-related operational risks*, such as industrial fires, supplier financial stress , or cargo theft from sources other than a cyber-attack (not during transport),
- *Natural disasters*, such as earthquakes, volcano eruptions, floods or wildfires
- *Transportation risks*, such as port congestion, cargo theft during transport from sources other than cyber-attacks, port infrastructure failure, vehicle derailment or accident, and vehicle malfunctions during transport,
- *Socio political risks*, such as civil unrest, law enforcement, or corporate social responsibility (CSR).

First, cyber-risks present a lower *latency* when compared to other types of supply chain risks. For example, natural disasters and its effects such as infrastructure unavailability receive public

news coverage, having thus a very low latency. The operational disruption form the natural disaster risk is thus quickly made known. Similar arguments can be made for disruptions from other supply chain risks such as industrial fires (Operational risks), port congestion (transport risks) and to a certain degree, civil unrest (socio-political risks).

Instead, the disruptive effects of cyber risks can go undetected for years until other performance problems arise. Such is the case of Stuxnet, where the high failure rate of centrifuges, and resulting rising average replacement costs gave way to the discovery of an attack that had been going on for at least 2 years (Zetter, 2014).

Second, cyber-risks present operational disruptions that are in some cases un-localized when compared to the *physical location* of other types of supply chain risks. For example, after natural disasters materialize the affected area is known. Road availability can be determined for a specific geographical area. A similar argument can be made for an industrial fire (operational risk), port congestion (transportation risk) or civil unrest (socio-political risk).

Instead, cyber-risks can lead to multiple geographies being affected simultaneously with a much higher complexity, such as in the case of the Wannacry ransomware where over 190 countries were affected (see Figure 91). Even in cases where the cyber-attack case is focused such as the Stuxnet attack, the attack also

caused damage in other locations in Europe and Asia (Zetter, 2014)

Third, cyber-risks present operational disruptions with a higher *complexity* when compared to other types of supply chain risks. The geographical effects of a natural disaster are restricted, e.g., only a certain number of roads are potentially affected. A similar argument can be made of an industrial fire or supplier financial stress (operational risk), and port congestion or vehicle failure (transport risks). The case is different for some socio-political risks, such as civil unrest, where the effects can eventually be very complex.

In the case of cyber-risks, this complexity is much higher. For the case of the Steel Mill cyber-attack, the complexity of the attack affected multiple plan systems sequentially, as was the case for the NHS ransomware attack and its ramifications. The complexity of cyber-attacks is represented in the different ways in which it affects the system, e.g., by replacing communications, disrupting communications, and by the greater number of communication streams in a system as there are agents in it.

Fourth, cyber-risks present a stronger perpetuity when compared to the other types of supply chain risks. A natural disaster presents a period when it affects operations (during the flood, earthquake or snow storm for example). Unless there are infrastructure damages as a result, operations can resume after the

natural disaster has ended. In the same way, and industrial fire (operational risk) is restricted by the existing material that can be burnt, a port congestion (transportation risks) will recede after some time due to market pressures for example, and a law that is being enforced is implemented. The combination of low latency and physical location results in focused actions being taken promptly to restrict the duration of supply chain risks other than cyber-risks.

On the other hand, a cyber-attack such as Leoni AG or Tesco Bank continue to operate as intended without losing its effect until specific countermeasures are implemented. No information was found in the gathered data of countermeasures for the effects of the cyber-attack, neither in Leoni AG nor in Tesco Bank. Actions taken after the incidents were made known focused on securing the information that allowed the fraudulent communications, and nothing was said about limiting the effects of such a fraudulent communication being received.

Fifth, cyber-risks present perfect replicability when compared to the other types of supply chain risks. Natural disaster risks are not considered as replicable. The same can be said of an industrial fire (operational risk), vehicle failure (transportation risk) or law enforcement (socio-political risk) as all develop on a case-by-case basis.

On the other hand, cyber-risk triggers such as ransomware, and computer viruses, trojans or worms replicate with a high level of fidelity.

Sixth, cyber-risks present a higher incidence of *interaction risks with respect to component risk* when compared to the other types of supply chain risks. Natural disasters disable affect the availability of roads and bridges, the components of the supply chain. A similar argument can be made of industrial fires or supplier financial stress (operational risks), and port infrastructure or vehicle failure (transportation risks).

In the case of socio-political risks, the disruptions are related to interactions between components of the system, e.g., supply chain and legislators (Law enforcement) or special interest groups and the company (CSR). For cyber risks in the case of the Leoni AG cyber-attack, it did not affect the information about the payment instruction (a necessary component for forgery) but rather affected the interaction between agents in the supply chain from this information. A similar case can be argued for the Steel Mill case, Tesco Bank or Stuxnet.

Seventh, cyber-risks higher *anonymity* when compared to the other types of supply chain risks. The origin of natural disasters is not anonymous, albeit sometimes providing limited reaction lead time.

On the other hand, the origin of a cyber-attack such as Wannacry or Stuxnet is not yet known, and it is unlikely that the origin of the attack will be identified.

Table 32 Comparison of risks along 7 dimensions

	Risk types				
Dimensions	**Cyber-risks to operations**	**Non-cyber-related operational risks**	**Natural Disasters**	**Transportation Risks**	**Socio Political risks**
Latency	High latency, sometimes years (e.g., Stuxnet)	Low (Industrial Fire) to medium (Supplier financial stress)	Low	Low	Low to medium
Physical Location	Can affect multiple locations (e.g., Wannacry)	Localized	Localized	Localized	Can have multiple locations (Civil unrest)
Complexity	Can affect many systems simultaneously	Limited complexity	Limited complexity	Limited complexity	low (Law enforcement) to medium (Civil unrest)
Replication	Perfect replication	No replication	No replication	No replication	Imperfect replication

	Risk types				
Dimensions	**Cyber-risks to operations**	**Non-cyber-related operational risks**	**Natural Disasters**	**Transportation Risks**	**Socio Political risks**
Perpetuity	Perpetual until counter-action; unless programmed to end	No replication. can be perpetual (e.g., supplier financial stress)	Limited	Limited (Port congestion) to long (infrastructure failure)	Limited (Law enforcement) to long (Civil unrest)
Component versus Interaction risks	Interaction risks	Component risk (e.g., supplier, infrastructure, cargo)	Component risk (e.g., supplier, infrastructure, cargo)	Component risk (Infrastrcture, vehicle)	Interaction risks
Anonymity	Anonymous unless explicit hacker declaration	Known perpetrator, traceable if not originally known	Known perpetrator, traceable if not originally known	Known perpetrator, traceable if not originally known	Known perpetrator, traceable if not originally known

7.2 Analysis of the systemic risk approach

The results presented from the application of STPA to an in-depth case is revelatory in different respects.

First, the results provide an increased "granularity" of the risk analysis. The structured STPA approach presented in the last section results in 119 different unsafe control actions (for a complete list, see Appendix section 11.2), which is equivalent to the same number of contexts that lead to a hazard. This is a list agreed by the members of the organization of the different ways in which the existing design of this supply chain can result in an unwanted event. In the terminology of the method, any of these 119 "*contexts*" can make a "*control action unsafe*", leading to a "*hazardous condition*" that can create an "*unacceptable loss*".

This approach builds from the original "disruption curve" by Sheffi & Rice (Sheffi et al., 2005), expanding the theory by uncovering mechanisms through which this behaviour over time is achieved in a supply chain after a cyber-attack i.e., cyber-resilience. The representation of information flows through a structured method with an explicit result, i.e., the information flow map, has been shown to enhance team productivity and effectiveness (Vennix, 1996; Sterman 2000).

The large number of contexts not being a rare outcome from an STPA analysis, and it is consistent with the findings from the applications of this methodology in other domains. However, these results originate two problems worth mentioning related to 1) the number of results and to 2) the nature of the results that are generated.

In regard to the number of results, if large these can be difficult to manage. The number of unsafe control actions can be understood as a greater granularity of the vulnerabilities present in the supply chain, yet this granularity also adds greater complexity to the management of these risks. It is therefore unlikely that a company will mitigate all the contexts uncovered though this analysis, for reasons that range from technical to political. Technical reasons are related to resources and timing, such as insufficient availability of resources to address and resolve all unsafe contexts, while political reasons are related to strategy and conflicts of interest, such as the unwillingness of supply management to expose so many new risks not considered previously for fear of appearing incompetent to upper management.

The nature of the results also differs from the results in the probability/severity risk analyses. This methodology does not assign a probability to the unsafe control actions or contexts.

Rather, these are identified from current supply chain design, and thus their probability of "occurrence" is 1: these design flaws exist in the system until these are solved, and as such can be exploited at any time.

7.2.1 Endogenous exposure

A probability calculation is next introduced, related to how likely an internal or external agent is to "make use" of any existing unsafe contexts resulting in an accident. This calculation of external threat likelihood is beyond this method as this reasoning is not endogenous.

The endogenous approach presented here is equivalent to an analysis that uncovers a great number of open doors in a system where you do not want external entry. These doors remain open until the organization decides to address the findings, and it is a management decision if either these design flaws are addressed, or the choice is to risk anyone foreign attempting to use any one of these doors.

Therefore, from the information revealed by this approach and consistent with a systems thinking framework, a way of quantifying this exposure is through the calculation of probabilities for the different hazards and accidents, thus providing management information to focus action on the ones

with the highest number of ways in which these accidents or hazards can be triggered.

This concept, of how exposed an organization is because of the structure it possesses, is being defined as "endogenous exposure":

Definition: "*Endogenous exposure is the property of a system of not fulfilling its objective because of the triggering, external or internal, of an internal design flaw*"

The calculation of the endogenous exposure is based on the "database" of contexts derived from the Unsafe Control Action analysis. This analysis can also be understood as a traceable register of the different sources for failure. If there are N different contexts identified through the analysis, the probability would be calculated as the number of applicable contexts for the specific hazard over the total number of contexts:

Equation 6

$$P(Hazard_i) = \frac{\sum_{j=1}^{N}((Context_j) \cup (Hazard_i))}{\sum_{j=1}^{N}(Context_j)}$$

A similar argument can be made for the probability of accidents. For the case of N different contexts and T different hazards, the probability of an accident materializing considers not only the pertinent contexts but also the hazards that correspond to that accident, thus, the probability is:

Equation 7

$$P(\text{Accident}_i) = \frac{\sum_{k=1}^{T}\sum_{j=1}^{N}((\text{Context}_j) \cup (\text{Hazard}_k) \cup (\text{Accident}_i))}{\sum_{j=1}^{N}(\text{Context}_j)}$$

The results for the data from this case are shown next. Table 28 shows the number of accidents, hazards, control actions and unsafe control actions identified for this case study. Table 33 shows the number of UCA for each accident, and the probability as the proportion of the total number of potential UCAs which actually lead to the specific accident, proposed in this work as an "*endogenous exposure*" measure for the organization.

Table 33 Unique UCA per Accident

Accident	CA	UCA	P(Accident)
Erroneous payment to supplier	16	93	78%
Product Integrity compromised	17	103	87%
Reputational Loss	15	92	77%
Erroneous arrival of product	18	110	92%
Product Loss	17	105	88%
Payment Loss	16	93	78%

In the same way, Table 34 shows the number of UCAs for the different hazards as defined for this case study. The probability

for each is defined as the proportion of UCAs of the total that lead to the specific hazard.

Table 34 Unique UCA per Hazard

Hazard	CA	UCA	P(Hazard)
Inability to perform physical transport	8	41	34%
Inability to initiate supply process	6	20	17%
Inability to confirm data transmission integrity	13	79	66%
Inability to confirm product integrity	10	44	37%
Inability to confirm data integrity	12	54	45%
Inability to confirm correct payment	8	33	28%

Additionally, four as the largest number of hazards assigned for a single UCA, as shown in Figure 5. This is an indication of the connection present in the system, and of the level of independence of the hazards from each other.

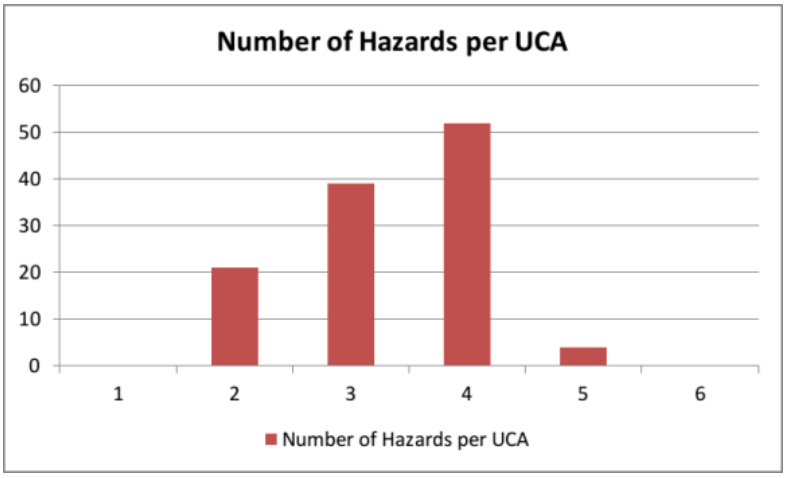

Figure 92 Number of hazards per UCA

7.2.2 System requirements from analysis

The analysis of requirements follows the system dynamics theory by considering dynamic behaviour is caused by a structure composed of stocks and flows. The analysis as shown in Table 35 results in the categorization of unwanted behaviours (UCA) as either related to problems of stock of information, of information flow, or of both.

Table 35 Information system requirements

SD UCA Categories	**Data (Stock)**	**Process (Flow)**	**Generic Type**	**Behaviour Description**	**Requirement**
Normal Operation	Correct	Correct		Process within the designed behaviour	No requirement
Data Corruption (Stock Problem)	Incorrect	Correct	GT1	Members of the system cannot identify each other unequivocally	Information system will include a process through which each system member can identify each other unequivocally
			GT2	Data for the process is changed without	Information system will include a data management

SD UCA Categories	Data (Stock)	Process (Flow)	Generic Type	Behaviour Description	Requirement
				members of the system noticing	process that will detect changes in data
Flawed Process (Flow Problem)	Correct	Incorrect	GT3	Process sequence advanced before confirmations are made	Information system will support the process sequence and confirmation milestones
			GT4	Process sequence understanding is different between the members of the system	Information system will continually communicate to all system members about the process sequence
Compound Problem	Incorrect	Incorrect	GT5	Wrong data is used for the process without members noticing	Information System will include communication data confirmation as milestone before data exchange between members
			GT6	Reaction times between members are not known	Information system will continually

SD UCA Categories	Data (Stock)	Process (Flow)	Generic Type	Behaviour Description	Requirement
				leading to untimely decisions	communicate all system members about required action dates.

7.2.3 Comparison of FMEA versus STPA performance

The process of developing the STPA analysis for the Procurement process was compared with an alternate method of risk analysis, the FMEA. This was possible, since the case company was in the process of updating its risk records to include cyber-risks. The comparison was done with respect to resources needed, risks uncovered and resulting requirements. The detailed results of the FMEA analysis were not disclosed by the company.

As is summarized in Table 36, the FMEA was a process required a reported four one-hour long meetings with 15 people per meeting, plus a 20 hour processing time. This process uncovered 48 risks for the procurement area in general with 15 risks that were specifically about cyber-risks. This compares with the 42 man-hours required for the STPA process, which uncovered 119 contexts for failure and 38 contexts that were about cyber-risks to the procurement area.

Where the comparison is particularly interesting is in the resulting requirements from the analysis. The FMEA resulted in 8 preventive measures for cyber-risks, and no design requirements were extracted from this process. In the meanwhile, the STPA process results in 28 preventive measures, directly related to some of the contexts that were described during the process, contexts that led to unsafe control actions. The STPA process also revealed 6 design recommendations (indicated as GT1 to GT6 in Table 35).

Table 36 FMEA – STPA performance comparison

Concept	**FMEA**	**STPA**
Resources Needed	260 man-hours	42 man-hours
Risks uncovered	48 overall risks 15 cyber-related risks	119 contexts for failure 38 contexts for cyber-risks
Resulting requirements	8 preventive measures 0 design recommendations	28 preventive measures 6 design recommendations

This result is not unexpected, as other experiences of STPA application for process analysis have also revealed many more unsafe contexts than other methods, including HAZOP and FMEA. For the particular case of this research this might be a result of several factors:

- *The structured process*. In contrast to FMEA, the STPA process has a structured way of both understanding the system, as well as of looking for the unsafe contexts. In the

case of FMEA, first the components of the system are identified and then, to identify the modes of failure, brainstorming sessions are held. Normally the identification of those components as well as the related information of probability of failure and severity of occurrence is quite time-consuming, particularly for cases where this information is highly dependent on a specific member of the organization that has the required information. This is the case for sensitive information such as monetary cost of failures. On the other hand, the STPA process starts by defining the system and its controllers with the existing information flows and control actions (CA). The contexts are then searched through a process that can be understood as “bounded brainstorming”, by concentrating the efforts of the people at the meeting in a specific domain of possible failures, for example “How could NOT executing this CA result in a hazardous condition?” This focused search is possibly part of the success of the method. Additionally, as the process is then repeated for different CAs and modes of CA influence (effecting the CA, not effecting the CA, effecting the CA too long or too early, and effecting the CA too much or too little).

- *The systemic thinking*. The unsafe contexts that are revealed through the process are not necessarily directly linked to the failure mode. But also context conditions are identified, as these are identified for their ability of creating a hazard, and not only the failure. For example, sending a purchase order to a supplier without checking the data of the supplier was identified as an unsafe way of effecting the control action "confirm PO with supplier". This is dangerous not directly because it creates an accident (in fact it was not detected in the FMEA), but because if a cyber-attack was to happen, the system would be open to a loss. This systemic approach to searching for hazardous conditions certainly contributes to a greater number of unsafe contexts.
- The *dynamic thinking*. The structured search for unsafe control action contexts considers a dynamic component, both through the "effecting the CA too soon or too late" and "effecting the CA too much or too little", as both are related to timing. Given the nature of the processes and control actions involved in the procurement process, the "too much-too little" component is not relevant. However, the "too early, too late" as a condition to search for unsafe control action contexts, does deliver some results that are invisible to the FMEA process, unless it comes out in the

brainstorming session. Yet, it has been documented that humans are particularly bad at understanding dynamic and special effects (Sterman, 2000), i.e., those effects that happen over time, or those effects that happen over distances, respectively.

- Going *beyond human failure*. A feature of systems thinking when evaluating risks, is that of considering design as the cause of errors made by humans, so rather than asking "why did a specific operator behave in this way", a question towards systems thinking would rather be "why would an operator in that circumstance have made that decision?". The answer to such a question would result in more contexts and design considerations.

7.3 Analysis of the dynamic modelling approach

The model in Figure 87, after being set in equilibrium, was tested for an initial disruption in the level of Exclusive IP stock, and different levels of marketing feedback. As an example, the sensitivity analysis for three parameters are shown next:

- The Customer adjustment time, or the time in months that customers return after a bad experience
- The Marketing Factor, which is the effect on demand in US$/Month resulting from every US$ spent in marketing

- The Promotion adjustment rate, which is the reaction time for adjustments in marketing budget after a disruption.

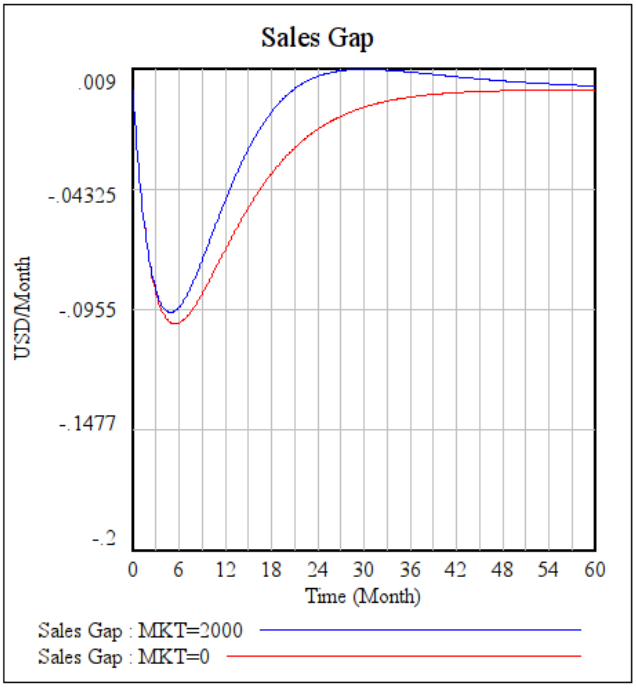

Figure 93 Marketing factor sensitivity

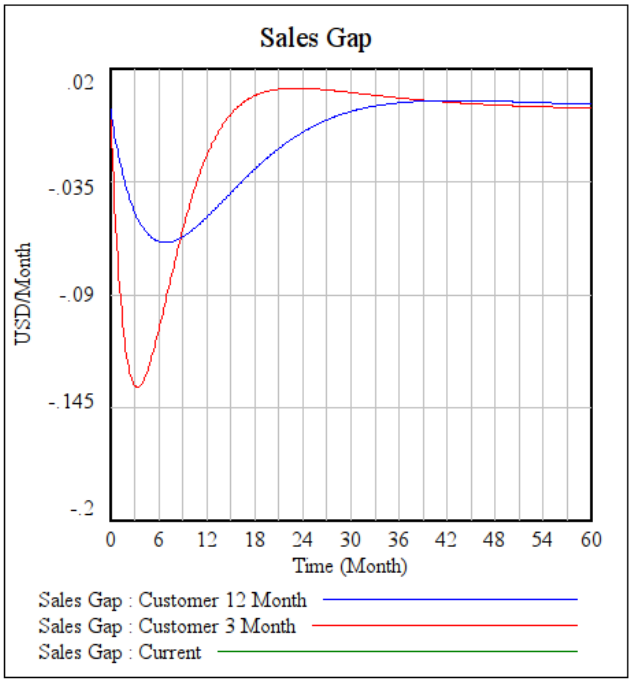

Figure 94 customer adjustment time sensitivity analysis

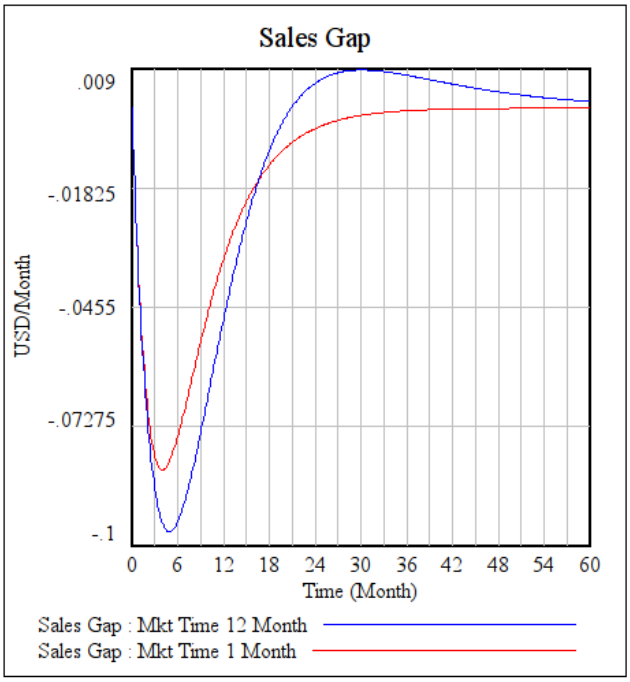

Figure 95 Marketing adjustment time sensitivity analysis

The values shown here are of the Sales Gap with respect to the Expected Sales. The general model behaviour can be explained by the balancing feedback loops present in the IP Stock adjustment and Customer Adjustment through marketing.

The model was not compared with the available data, as the model that includes all the medium and long term feedbacks resulting from the case description have not been included in a quantifiable model. The values if the Sales Gap, although following a similar curve than the one obtained from company data (see Figure 72), the values are much smaller than the ones

reported. This is the result of both the pending inclusion of factors that decreased the sales post-disruption, such as the loss of contracts and loss of sales due to product safety problems derived from the IP Theft, and the inclusion of costs derived from the use of PR, cyber-security and legal services.

However, despite delivering limited results from the simulation, the process of simulation, the process reveals a series of problems and advantages.

The problems have relation with the quantification of the variables, and the sequential construction process of the model, and the calibration of the model by comparing its behaviour with an observed, measures variable.

The advantages of the process relate to the sequential identification of variables and their relationships through the casual loop diagram and the hierarchical control structure. Therefore insights and behaviour development such as the description of the feedback loops detailed in section 6.4, can explicitly represent information about the cyber-attack, serve as an explicit representation of an agreed system structure, and guide the focused building of a simulation model to answer specific questions related to an attack.

7.4 Answer to research questions

The analyses detailed in the previous section are used in this section to provide answers to the research questions as detailed in Table 18.

7.4.1 Answer to research sub-question 3

The research sub-question 3 refers to the nature, i.e., the particular characteristics, of cyber-risks with respect to other supply chain risks.

Research sub-question 3: how do cyber-risks cause operational disruption in supply chains and how does this differ from other supply chain risks?

The process of answering this question, as indicated in Table 18, is separated into three sub-questions:

- First, an exploratory that analyses the events of operational disruptions caused by cyber-attacks that have been recorded beyond published literature, which originates research sub-question 3.1. *RSQ3.1: What events of operational disruptions caused by cyber-risks have been recorded?*
- Second, a more descriptive aspect where the events that are found are used to describe how the operational disruption is caused, which originates research sub-question 3.2.

RSQ3.2: How have these events resulted in operational disruption?

- Third, an aspect that is more evaluative that compares disruptions from cyber-risks to disruptions by other supply chain risks, *RSQ3.3: How do events from cyber-risks differ from events from other supply chain risks?*

The results of this part of the research are found in chapter 4, and based on those results, the following answers to these research questions are suggested.

RSQ3.1: What events of operational disruptions caused by cyber-risks have been recorded?

The events of operational disruption are being recorded continuously in different media beyond published literature, as evidenced by the number of reports of cyber-attacks that could be retrieved through the methodology applied in this thesis, 2425 reports, despite this methodology not being exhaustive. All the cyber-attack reports that were gathered are related in some way to the loss of data, either

The reports appear first in newspapers or blog websites specialized on the topic of hacker attacks, and the information they contain is of variable depth and quality. All of the reports that

were found mention at least three things, the company industry where this attack happened, the type of attack (e.g., data loss, operational disruption), and a quantification of the disruption, be this in monetary value, or quantity of loss data, for example.

These events are then reported with some lag by newsletters, and specialized consultants such as software security companies. Finally these events are summarized by specialized government agencies and specialized consultants, business consultants and insurance companies.

The times of record for the cyber-attacks, ranging from the same day to one week after. The sooner the report the less information that was made available about the mechanics of the attack.

The data gathered included a range of reports with a reporting lag from the incident occurring to the date of the report that ranges from hours to months. In the detailed sample that was gathered, 3% of the reports were connected with some type of operational disruption, and as was seen in the case groups presented in section 4.2, all cases originate in the loss of data. Only 1% of cases of intellectual property loss was seen in the sample. Given that the research process of archival research did not intend to be

exhaustive, these number provide an instance of the relative quantities.

There is a dispersion in terms of the countries to which the attacks in the sample are directed, most of the ones in the sample directed towards the US and UK, with India in a distant third place.

This dispersion is not generalizable, and might be related to the method of data gathering, including sources and language of reports for example.

RSQ3.2: How have these events resulted in operational disruption?

The cases that are presented in chapter 4 are categorized according to the disruptions these cause to the supply chain. The five identified categories are 1) active theft of resources, 2) passive theft of resources, 3) active theft of products, 4) active disruption of operations, and 5) passive disruption of operations.

Each of these categories present a distinguishing set of characteristics related to how the supply chain disruption is caused, as well as other categories that are similar and which distinguishes cyber-risks as a group from other supply chain risks. Some common features are found in the gathered data:

- All the cases are dependent on stolen proprietary data of some sort: 1) directly, as in case of cyber-attacks as a result the loss of data, or 2) indirectly, as in case of cyber-attacks that have an operational disruption as outcome from the use of proprietary data that had been stole previously.
- All the cases have a mechanism of deception, for the replacement of expected communication streams by fraudulent ones, either 1) to another member of the supply chain, or 2) to a member within the organization,
- All the cases have a mechanism of undue influence, for the creation of legitimate but wrong communication streams either 1) to other members of the supply chain, or 2) to members of the same organization,
- Most cases have a mechanism of reward, for the hackers in the form of either in the form of 1) organizational resources such as money or IP, or 2) products from suppliers to the organization.
- The progression of these mechanisms is very consistent, identified as 1) the unauthorized use of proprietary data to follow a sequence in the mechanisms of 2) deception, 3) undue influence, and 4) reward. This is likely not a linear process, but rather a cyclic process, as the reward is the incentive driving data theft.

Figure 96 shows an example of this sequence for some example cases.

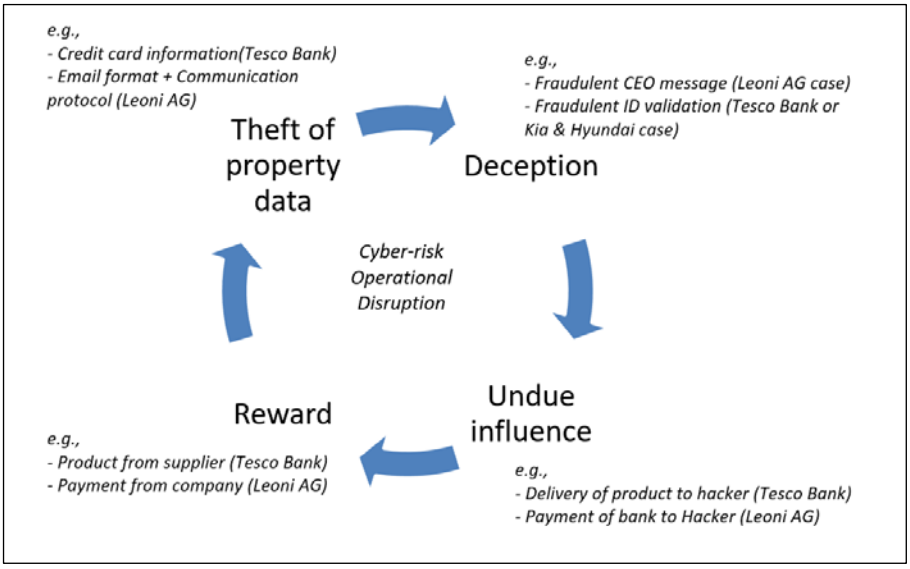

Figure 96 Cycle of disruption

Finally the aspect relating to the difference between cyber-risks and other supply chain risks, is contained in research sub-question 3.3.

> *RSQ3.3: How do events from cyber risks differ from other supply chain risks?*

Differences between cyber-risks and other supply chain risks are identified along dimensions of latency, physical location,

complexity, replication, perpetuity, anonymity, and component versus interaction as main driver of the risks.

Cyber risks are compared with other supply chain risks grouped according to categories of 1) Non-cyber-related operational risks such as industrial fires of supplier financial stress, 2) natural disaster risk such as earthquakes or floods, 3) transportation risks such as port congestion or vehicle failure, and 4) socio political risks, such as civil unrest or corporate social responsibility risks.

Table 32 shows a detailed account of the differences between the dimensions and categories of the analysis, and the practical implications are summarized in the following table:

Table 37 Cyber-risks vs. Physical risks in supply chains

Dimension	**Events from Supply chain cyber risks**	**Events from other supply chain risks**
Physical location	Physical location is irrelevant	Physical location is relevant
Anonymity	Anonymity is common	Anonymity is uncommon
Complexity	Unlimited complexity	Limited complexity
Latency	Can go undetected for a long time	Cannot go undetected for a long time
Component versus Interaction	Mainly interaction risks	Mainly component risk
Replication	Perfect replication	Difficult or imperfect replication
Perpetuity	Events will continue until counteracted	Events mostly have a duration

7.4.2 Answer to research sub-question 4

The research sub question 4 refers to the use of systems thinking to mitigate some of the gaps that were detected during

the systematic literature review for managing cyber-risks in the supply chain.

Research sub-question 4: how can a systems approach be used to mitigate compartmentalization, static frameworks and historical dependence for managing cyber-risks in the supply chain?

This question was separated in two parts, as shown in Table 38, to extract insights from the application of two systems thinking approaches for the management of cyber-risks, one for the evaluation of risks, and another for the simulation of the resilient response to cyber-risks.

Table 38 RSQ4 and derived research sub-questions

Research question		**Explanatory**	**Evaluative**
RSQ4	**How can a systems approach be used to mitigate compartmentalization, static frameworks and historical-dependence for managing cyber risks in the supply chain?**	RSQ4.1a.- How can a systemic risk analysis approach mitigate compartmentalization, static frameworks and historical dependence for managing cyber risks in the supply chain?	RSQ4.1b.- How does a systemic risk analysis approach compare to established risk analysis methods?
		RSQ4.2.- How can System Dynamics simulation mitigate compartmentalization, static frameworks and historical dependence for managing cyber	

		risks in the supply chain?	

Next, answer to these derived sub-questions and then to sub-question 4 are detailed:

> *RSQ4.1a: How can a systemic risk analysis approach mitigate compartmentalization, static frameworks and historical dependence for managing cyber risks in the supply chain?*

The process of systemic risk analysis as structured through the STPA process, addresses compartmentalization, static evaluation of risk and historical dependence of the risk evaluation in specific ways.

The *compartmentalization* is addressed through the process by which the unsafe control actions are identified. The process is similar to the traditional event tree analysis and branches out from the undesirable outcomes in this case the list of unacceptable losses shown in Table 25. However, in contrast to the event tree method, the STPA process continues with a process of structured enquiry by first defining the relevant system of controllers and

control actions, to then identify these dangerous conditions by assuming four instances when this dangerous condition might arise, this is, either through:

- A controller executing a control action in its domain
- A controller not executing a control action in its domain
- A controller executing a control action in its domain too early or too late, or
- A controller executing a control action in its domain for too long or too short a period.

These options do not compartmentalize the areas of the system that are involved. For example, the UCA (unsafe control action) of "Buyer executes instruction of supplier payment before product validation" involves the areas of finance, warehousing and purchasing. Additionally, the level of aggregation selected for the analysis will condition the hierarchical level at which the controllers and their actions are being considered and the process of finding UCAs required by the method, does not compartmentalize at any level of hierarchy or aggregation.

The *static framework gap* is addressed by the STPA method by including time in the analysis of UCAs from the perspective of 1) executing UCAs too soon or too late, and 2) executing UCAs for too long or too short a period. These conditions reveal contexts

which are time-related. For example, the UCA "Bank executes the transfer of funds to the supplier before the correct payment amount has been confirmed" contains a sequence of activities, this is it is necessary to confirm payment amount before executing the control action. This results in a requirement of confirming monetary amounts throughout the payment process, requirement that can be fulfilled through a number of alternatives.

The *historical independence*, from its application to the case study, is understood as only partial. The aspects that are history-independent include:

- The operating requirements, i.e., the accidents and hazards of the system, as these are obtained from management expectations,
- The structure of the system that is required for unsafe context analysis, i.e., controllers and control actions, which are a result of the mental maps about the organization, and
- The identification of unsafe control actions through a process of imagination.

On the other hand, the historical-dependence of the STPA process, is related to:

- The cycle of the process as illustrated in Figure 35, inasmuch as the next cycle of system definition will be

dependent on the outcome requirements from a previous cycle of analysis. This is not a limitation, but rather a feature of the method. When history-dependency was identified as a gap during the literature review, this dependency was seen as a gap in cases where there was no previous experience from which to extract data for analysis. In the case of STPA, the data is the system structure and the dependency is the updating of this structure with the requirements from previous analysis cycles. See section 2.9.2 when the gap type 2 from the SLR is described, related to the methods used cyber resilience analysis.

- The identification of unsafe contexts of operation, when these identification is derived from experience. For rare or very specialized systems, experience about the potential ways in which the structure of the system can lead to an unsafe context of operation that is undetectable with this experience.

As a *corollary to answering question 4.1a*, the evidence gathered in the thesis reveals that the STPA systemic risk analysis method addresses compartmentalization and the dynamic nature of the systems being managed, and provides partial time-independence to analysis.

RSQ4.1b compares this method to other established method:

RSQ4.1b: How does a systemic risk analysis approach compare to established risk analysis methods?

The results from the application of the STPA method were compared to the results from the FMEA analysis, as described in section 7.2.3. The evidence shows several advantages of using a systemic risk analysis for the evaluation of cyber risks, related to

- Resources needed for the risk assessment in terms of man-hours needed, as the STPA process needed 16% of the resources needed by an FMEA process for the same end, i.e., identifying cyber-risks,
- Number of failure contexts uncovered, as the STPA process uncovered 153% more cyber-risks (148% more overall risks)
- Number of design recommendations, as the FMEA did not reveal design recommendations related to cyber-risks,
- Number of preventive measures, as the STPA process revealed 2,5 as many preventive measures as the FMEA process of the same purpose,
- Structuring of the process and incorporation of systemic and dynamic thinking.
- Going beyond human failure for recommendations.

As a *corollary to answering RSQ4.1b*, a systemic risk analysis method evidences several promising features in its application to cyber-risk analysis in a supply chain. Consideration should be had that these features were uncovered through the revelatory study presented in this thesis, and will require further evidence to consolidate these revelations as definitive characteristics of the method.

The final research sub-question is concerned with the use of dynamic simulation:

> *RSQ4.2: How can system dynamics simulation mitigate compartmentalization, static frameworks and historical dependence for managing cyber-risks in the supply chain?*

The process of dynamic simulation as structured through the system dynamics method, addresses compartmentalization, static versus dynamic concerns as well as historical-dependence of the risk evaluation in specific ways.

The *compartmentalization* is addressed through the process by which the modelling is progressed, as the causal loop

diagramming, the hierarchical control structure and the stock and flow diagram all consider a trans-organizational approach.

- The casual loop diagram, as shown for example in Figure 75 originates from the identification of the relevant variables involved in the system, and related to the behaviour that is at justifies the model, this is the reference mode. These variables are not related to any part of the system specifically, as it is the causal relationships that originate the connections. The only compartment that is considered in the process is the system itself, this is, the limits within which the close causality is explored.
- The hierarchical control structure, such as the one represented in Figure 86 goes a step further, as it identifies the "*sectors*" within the system between which the connections occur. It builds on the causal loop diagram for the case developed in this thesis, but I can be the starting point of the analysis, as all causal loops are contained in the hierarchical control structure as well.
- The stock-and-flow diagram, such as the one shown in Figure 87 do not consider compartments either, and are restricted to explaining the system structure and behaviour by generating a causally closed model

The *static versus dynamic* concerns are addressed by the dynamic models explicitly, despite not all of them in the same way.

- The model least concerned with dynamics is the hierarchical control structure, as it represents the sectors in the system, and the relationships between these sectors, for examples, as it has been illustrated in Figure 77 or Figure 80, for example. This structure does not identify time in any of its definitions, and its application is to 1) order the concepts involved in the system definition for subsequent stock-and-flow modelling, concepts mentioned in section 6.5, and 2) to serve as a more familiar introduction to the modelling process to laymen in an organization, due to the use by the hierarchical control structure diagram of existing areas and communication process that can be identified by members of the system.
- The causal loop diagram, despite not quantifying the variables it represent, it lays out the circular causality structures, i.e., feedback loops, that explain the evolution over time of the variables of interest, in this case the profit and the sales.

- The stock-and-flow diagram is based on the modelling of its structure over time, and it is thus intrinsically a dynamic process.

The *historical dependence* of the dynamic modelling process is variable depending on the dynamic model that is used:

- Both the Hierarchical control stricture and the causal loop diagram entirely rely on the present structure of the system that is being modelled, and as such depends in history only inasmuch as it requires the extraction of mental models from members of the organization, mental models which are formed by experience.
- The stock-and-flow diagram, despite being constituted by the structure of the system being modelled, when it is used for predictive or prescriptive purposes, its calibration is achieved by the quantification of exogenous variables to the system. For example, in the case of the model represented in Figure 87, for example, the “marketing factor” or the “Cobb Constant” have to be quantified. Some of the techniques that can be used to quantify these variables consider past history. However, other processes exist that can achieve this quantification relying on the historical information concerning the reference mode of interest. These quantification processes not discussed in this thesis,

but include maximum likelihood methods, bootstrapping methods, or methods of simulated moments (Rahmandad et al., 2015), for example.

As a corollary to answering RSQ4.2, the dynamic modelling method provides an explicit, structured process to collect information contained in mental models from members, and formal information in a supply chain. This process addresses compartmentalization, are dynamic, and do not rely on historical information.

7.4.3 Answer to Main Research Question

The answers to the different research sub-questions presented in sections 2.8.1, 2.8.2, 7.4.1, and 7.4.2 provide information to answer the main research question (see Figure 2 for an overview of this structure of enquiry):

> *RQ: How can cybersecurity and cyber-resilience be managed in the global supply chain?*

Cyber-risks differ from other supply chain risks in several fundamental dimensions. For example, cyber risks can have higher levels of complexity, geographical dispersion or be more difficult to detect than other risks to the supply chain Additionally, the risk assessment methods that are available for supply chains

to prepare and react to cyber-attacks have shortcomings, for example, through their dependence on historical data or relative neglect of the dynamics of an supply chain when understanding cyber resilience. Therefore, after the analysis in this thesis it is no surprise that negative effects from cyber-attacks continue to manifest as operational disruptions, and both the gaps uncovered through the SLR and the particular characteristics of cyber risks provide a foundation to assert that cyber-attacks will continue to occur:

Cyber risks rely on the existing structure of a supply chain, particularly the proprietary information, communication channels, and established procedures between supply chain partners.

As a result, management processes that are suggested for cyber risks, consider both this particular nature of cyber risks, as well as the process that cyber risks enable for attacks to convert to operational disruption.

The management of cyber risks in a global supply, as a result of the evidence gathered, will therefore benefit from considering:

- An approach that understands *cyber-risks as different from other supply chain risks* (see section 7.1.2) in their complexity, geographical dispersion of disruptions, difficulty of identification, persistence, and intrinsic

anonymity, for example. In contrast with other supply chain risks that could be managed through protection, cyber-risks evidence the need to understand and design the supply chain structure, as it is this structure that is being used by hackers to disrupt (see section 4.2).

- An *un-compartmentalized approach* to the identification of risks. This exposes conditions that are not immediately leading to a cyber-risk materializing as a disruption, but rather set the stage for this disruption to be likely. These "*distal*" causes are invisible to traditional methods that operate through the causal chain approach, but can easily be identified through system-thinking based methods (see sections 5.2 and 6.4).
- An approach from management team to *designing the reaction of the supply chains that are needed*. This approach benefits from the simulation of ranges of operation and structures that better result in the required behaviours (see sections 6.6 and 7.2.2), and as a result requires looking inward to the structure present in the supply chain as source of threats, instead of looking outside the supply chain for the identification of threats (see section 7.2.1).
- An approach that will take into consideration the use of *modular design* to manage increasingly complex systems,

through the system definition as a causally closed set of components and relationships that result in the observed behaviour (see section 3.2.3),

- An approach that will *not depend on history of attacks* for the evaluation of cyber-risks, as technologies such as IoT (Internet of Things) will introduce vulnerabilities that are as yet unknown (see section 7.4.2). The methods based on systems thinking, by considering the structure of the supply chain as the source of risks, has a focus on supply chain design irrespective of the external threats.
- An approach that will acknowledge *the strength in mental models*, both as source of information about a cyber-physical and socio-technical system, but also as source of difficulty to change. The system-thinking based processes developed in this thesis serve as a platform to channel this change. The required changes include for example, the migration from risk assessment to resilience assessment (see section 3.2.1, 3.8.3 and 3.9.3).

7.5 Implications for supply chains

The answers that have been given to the research questions in this thesis have different consequences for industry and in particular to supply chains.

7.5.1 Updating the threat paradigm

There is a necessary, yet troubled migration from risk to resilience management for the case of cyber-risks. Linkov et al. (2013a) particularly highlights the "*dominant paradigm of quantitative risk assessment for system design and management*" and how these pervasive concepts from risk "*have encroached themselves in the understanding of resilience*".

Since resilience has a wider scope, and considering that every risk analysis is in reality a resilience analysis, albeit limited, there is a need to incorporate new tools that are clearly identifiable from those directed to merely quantitative risk analysis. This work is proposing two approaches towards that end: systemic risk analysis, and dynamic simulation.

The increasing reporting of malware with the potential of disrupting operations has different implications for the functioning and development of supply chains.

7.5.2 Cyber-threats are the new normal

Malware reports expose what is probably the tip of the iceberg of a whole ecosystem of programmers developing software to exploit supply chain vulnerabilities. Different communities related to the development and commercialization of vulnerabilities have been documented; groups that show

increasing specialization (Leveson, 1995; Zetter, 2014; Bartlett, 2015; Goodman, 2015).

Additionally, the extent of these vulnerability-exploiting communities and the incentives behind the perpetrators is still diffuse or undetermined. Therefore, expecting to understand attacker incentives before a decision is not an efficient option due to 1) the difficulty of determining those incentives, and 2) irrelevance of attacker incentives when designing how a company should react and recover from an attack.

Instead, available resources, their deployment and control strategy largely determines the undesired operational effects of a cyber-attack irrespective of the attack source. For example, vulnerabilities can be “exploited” unwillingly by unsuspecting members of an organization, case where there is no intention to harm.

Given the connectedness of the information network underlying physical processes, a protection criteria based on the direct effects of a vulnerability is incomplete at best and ineffective at worst, since in a connected network, vulnerabilities have an undesirable effect through the weakest link in the organization: connections rather than components become paramount (Leveson, 1994).

7.5.3 Risk analysis is risky

Risk analysis not only uncovers vulnerabilities, but makes them known. It is as such a double edge sword. The unsafe control action analysis detailed in section 5.2 both results in requirements for the elimination of hazardous contexts (see Table 35), but at the same time exposes in detail different ways in which the current system can be driven to an unacceptable loss.

7.5.4 Modular control versus centralized control

The concept of hierarchical control structure that has been used both in the systemic risk analysis and in the process of arriving to a dynamic simulation model has implications for the management of complex systems.

- First, a systems approach with the consideration of hierarchical control structures, points towards the design of self-regulated modules, providing a base for de-centralized control in complex supply chains. In contrast to centralized control, the modularity achieved by defining causally-closed systems, allows the replication of these modules with similar sub-systems, for example, by making modular requirements for auto-regulation that is applicable to a group of similar suppliers.

- Second, the control of the organization can be designed and thought in terms of hierarchies. Although this has been present to some degree in organizations through the use of area managers, a hierarchical control structure can allow for the conscious design of such a structure,
- Third the modular design can be pursued at different levels of aggregation, as the defined causally-closed system might be a production unit or a plant.
- Fourth, the paradigm change that is required for managing a complex system from the point of control structures, requires that the some of the education that is currently delivered to prospective be adjusted to consider systems thinking, analysis and design as a core competency.

7.5.5 Managers as designers

Anderson (1993) argued early on that it was management problems and not necessarily hardware problem that are many times the source of the vulnerabilities in systems that have implemented IT Systems. He highlighted the particular problems faced by cryptographic systems regarding feedback about their failures. In an analogy, Anderson compares the information other developers have access to when the systems they are designing fail, such as in the case of an airplane. In that case, when there is

a crush, it is normally front-page news, with investigators studying the scene, and a wide variety of actors processing the information at a technical and social level, such as the carrier, the manufacturer, and the local aviation authority. This constitutes an "*institutionalized learning mechanism*" which is absent in the case of cryptosystems, and probably other security systems.

The lack of this learning mechanism in the case of security systems results in the same mistakes being made over and over again, with the advancement of attribution for problem solving advancing at a slow pace (Anderson, 1993; Rid et al, 2015). This risk is only increased by initiatives such as the outsourcing of IT capabilities (Earl, 1996).

Shutao et al. (2009) lays out derived suggestions that managerial skills and partner coordination and support are significant drivers in the deriving value of the use of IT in supply chains, and that much of that value comes from "fitting the pieces together" beyond only having the available technological resources. Shutao and his team analysed three key resources driving performance improvement in supply chain by the use of IT, namely backend integration, managerial skills and partner support. Of these, and based on case studies, managerial skills presented the strongest correlation performance improvement,

understood as process performance and competitive position, as is shown in Figure 97.

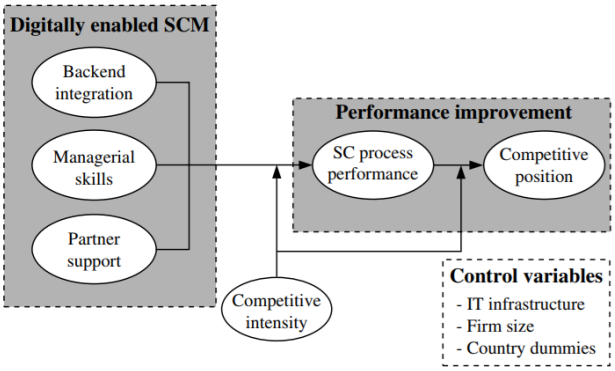

Figure 97 Resources in IT enabled SC (Shutao et al., 2009)

Managers therefore have a function that largely exceeds operative functions, such as organizational design (Keough et al., 1992). The systems thinking tools used in this thesis provide a foundation for design.

7.5.6 Non-historical risk analysis methods

The speed with which cyber-attacks are occurring, and the slow reporting cycle in accepted information sources (see analysis in section 2.9.1) point at least towards to possible scenarios. Either:

- Academia drifts away from practitioners in the study and effective management of cyber-risks as academia is not able to keep up with the speed required by practitioners, or

- Academia explores methods and processes to respond in the time and depth required by practitioners.

The evidence gathered in this thesis points both to a need in academia and industry to 1) increase the speed of reporting and to 2) develop methods which are less history-dependent (see the analysis in section 2.9.2).

The use of the either systems thinking based methods shown in this thesis result in a process that is less history-dependent (see section 7.4.2).

7.6 Implications for academia

7.6.1 Alternative ways to obtain information

Findings from the SLR indicate that the access to information about cyber-attacks is very difficult, driven by incentives that continue to exist (see section 2.9.1). A result of this, is that in order to access this information, alternate ways of accessing this information must be explored.

Although the relevance of cyber-risks to the supply chain is understood (Hult et al., 2014), and it is clear that gathering data of cyber-attacks has the potential of decreasing organizational costs and of lowering the risks of cyber-attacks, this data gathering has been marginal and incomplete (Glaessner et al., 2002), as there are

important hurdles which are keeping back organizations from contributing to this data collection. These hurdles have been categorized as fragmented information (Anderson et al., 2013), incentives towards non-disclosure, and inability of risk quantification (Cashell et al., 2004).

The incentives towards non-disclosure are real economic incentives experienced by companies that lead them to withhold information of cyber-attacks. The costs from a disclosure that has been made public may take different forms, such as impact in financial markets, effects to the reputation and confidence of an organization, litigation concerns related to the cyber-attacks, liability concerns derived from the attacks, agent effects such as job security, and signals to potential attackers (Cashell et al., 2004). These costs of disclosure have been summarized the following table.

Table 39 Costs of disclosure for cyber-risks

Disclosure cost name	**Description**	**Example**
Impact in financial markets (Signal to market)	Financial market such as stocks and bonds react negatively to news of cyber- attacks. Additionally, banks and potential lenders can rank organization as being more risky die to a previous cyber attack	The World Economic Forum has highlighted that organizations experiencing a cyber-attack have lost as much as 7% of their market value even before making a cyber-attack public.
Effects to reputation and confidence (Signal to supply chain)	News from a cyber-attack affect the reputation or brand value of the affected organization, or causes customers to loose trust in the product, opening up an advantage for competitors.	
Litigations	When the consequences of a cyber-attack are disclosed, any number of supply chain agents, customers, investors or shareholders may use the	

Disclosure cost name	**Description**	**Example**
	legal system to attempt the recovery of damages. This may open up a pattern of negligence with effects on the reputation.	
Liabilities	The investigation of a documented cyber-attack may result in economic sanctions for the company due to its accountability, or standards for safeguarding patent and customer records. The latter may also result in litigations with customers defending the privacy of their information.	
Agent effects	Any effect involving a person having a role in the affected organization, where the personal benefit and the organizational benefit are at conflict, and	Organization members responsible for the cyber-attack have incentives to conceal the attack for fear of losing their jobs.

Disclosure cost name	Description	Example
	where the personal benefit option is taken.	
Signals to potential attackers	The public disclosure of a cyber-attack may signal other potential attackers of high organizational vulnerabilities towards cyber-risks	

It is therefore imperative for academia to develop ways of circumventing or counteracting these perverse incentives in order to increase data gathering.

7.6.2 Evaluation of sources of research data

As indicated in the introduction of this thesis, cyber-attacks that are occurring to organizations with a frequency and speed such, that some of the information from these events has not yet been integrated into journals, and it seems unlikely that this will occur in future with enough promptness to be used in current research (see analysis in section 2.9.1).

Authors have proposed ways of evaluating website content for their validity (Stoker et al., 1994; Banos et al., 2013). The

objective of this evaluation is to establish if the information required by the research comes from an adequate source. For example, a widely used framework for the evaluation of sources of information is the CRAAP framework, also known as the CRAAP test (Blakeslee, 2004; Wichowski et al. (2012) which proposes:

- C: Currency, i.e., how recent is the source of information, in terms of when it was written, and when it was last revised.
- R: Relevance, i.e., whether the information provided by the source is within the scope of the project for which the information is gathered.
- A: Authority, i.e., whether the source of information has a visible author, the author credentials and website credentials, as domains such as "*.edu*", "*.gov*", "*.com*" or "*.org*" may have different authority levels.
- A: Accuracy, i.e., whether the information source strives for reliability, truth and accuracy.
- P: Purpose, i.e., the reasons why the information from the source was published, such as to persuade, to entertain, to provide facts, or to teach.

Therefore, an implication to academia from the results of this thesis research, particularly the method described in section 3.7, and its results as described in section 4.2, is that the research process needs to include new sources of data in a way that is accepted by the scientific community.

7.6.3 Dynamics in the case study process

Case study method, or the in-depth inquiry into a topic or phenomenon within its real-life setting (Case studies in general, and particularly about resilient response in supply chains from sources such as a cyber-attack, lack a focus on the dynamic response for the case being described despite proposals about the complementarity of the case study method and a system dynamics approach (*Papachristos, 2012).*

The use of case study in this research reveals the shortcoming in current case study process descriptions and its incomplete understanding of "*dynamics*" during the established data gathering and analysis processes. The implication to academia as a result of the results in this thesis is an opportunity for collecting the dynamics as well as the systemic implications of a case (see sections 3.8.3, 3.9.3 and 6.4) to enable distal causality analysis, circular causality analysis and dynamic simulation (see section 6.6) of a cases where reaction over time is relevant.

7.6.4 Consolidate cyber-resilience research community

The multiple unconnected sources found the SLR about cyber-resilience (see Table 12), as well as the very few frameworks that had any connection to resilience frameworks (see analysis in section 2.7.4) point to the lack of a established community for the research of cyber-resilience in the supply chain.

Given that the cyber-threat is not likely to decrease, the implication to academia is that a consolidated research group on cyber-resilience can better drive a structured research process.

7.6.5 Research methods applicable to other attack types

The dynamic research methods applied to cyber-risks and cyber-resilience, are in every way applicable to other types of risks that are experienced by organizations. Given the particular characteristics of cyber-risks, it is that a structural approach is required, while other risks such as financial or environmental, having physical restrictions in the complexity these can reach, can be treated through localized strategies, an organization would nevertheless benefit from understanding the structural design that is exposing it to these risks.

7.7 Study limitations

The dynamics simulation was based on a system dynamics model of the IP generation process, starting from a case study analysis of the event. The aspects that are discussed in this section include the way in which the case study data was gathered (including the hurdles for data gathering and the special nature of the data that was gathered), as well as from the results that were obtained through the simulation and the implications these results have on practitioner

7.7.1 External validity of systems-thinking methods

Despite measures are taken in this thesis to address the validity of the results (see section 3.10), particularly the external validity of the results is not robust. The approach of this research is a revelatory approach. By using systems-thinking methods to specific case studies, the characteristics of the tool were analysed to identify the degree to which these addressed the method gaps revealed after the SLR.

It is therefore a limitation of the process shown in this part of the thesis. This limitation does not restrict answering the research questions that give rise to the research, as the questions deal with the method.

7.7.2 Case study limitations

The case study presents a practical instance where to develop the system dynamics method starting from an example of a cyber-attack actually having affected a company. The case study method relies on the information provided by the case company, and calibrated against values found in literature. Different aspects can be identified as limitations:

- Bias limitations. The information source contains bias. The effect of the cyber-attack that resulted in the loss of IP is a self-reported value, which could be subject to manipulation, for example, as a way to argue other negative results as derived from the cyber-attack, while these might have other origins. Despite this effect is not something this thesis sets out to measure, the general behaviour of the performance measure after a disruption (in this case the sales and profit gaps) agrees with the behaviour seen from the simulation method, and can be directly traced to and explained from the structure that was developed for this model.
- Dynamic-focus limitations. The information as presented does not collect information about dynamics, i.e., how variables in the system change over time, what accumulates versus what flows in the system, and what are the feedback loops. The dynamics for the case is rather inferred from the

incident descriptions. This is not an uncommon approach, particularly with groups that do not have systems thinking training (Vennix, 1996)

7.7.3 Systemic risk analysis

It has been argued that despite its ability to identify and structure contributing factors to "*accidents*" when dealing with complex systems, the use of systemic risk analysis unfortunately has some drawbacks that have to be considered for any current application of the method (Bennett, 2016):

- Systems thinking-informed analyses are *intellectually demanding*, partly because of the paradigm change it requires to understand and model a problem by looking at aggregate effects, hierarchies, constraints and process models, (Leveson, 2011)
- Systems thinking-informed analyses can be potentially time consuming, particularly if these are attempted without the proper training or guidance. However, as it has been indicated in this thesis, the time required for this process once a basic knowledge for implementation has been attained, is substantially lower than other established methods.

- Systems thinking-informed analysis can be unpopular with interested parties such as politicians, constituents, managements, shareholders, regulators or journalists, as an endogenous causality method reveals that it is the decisions of the members of the system that are likely to drive an unwanted behaviour. This is an reason for the recommended use of group building techniques during the process (Vennix, 1996; Leveson, 2011)
- Bennet (2016) has mentioned systems thinking-informed analysis as more costly, although no evidence has been provided of where this extra cost actually comes from. No costs were calculated for this thesis, despite the finding that the resources needed for the analysed case, were lower.

7.7.4 System Dynamics modelling

Despite the advantages that a system dynamics approach offers to organizations, it has several important hurdles to overcome before its application is more widespread. These difficulties have to do with the application of the method and with the method itself.

The application of the method and the motivation to implement it are at odds, as:

"In a normal corporate setting, the window of opportunity for introducing and understanding their dynamics is very narrow. An organization that has no problems and thinks it is doing just fine doesn't have really any motivation to go out and look for trouble it has not experienced. Then it reaches a point where it sees the handwriting on the wall, and it might be amenable to try to understand the nature of their problems, but it may be a very short time after that when the crisis is so deep that there is no time to study it, and in fact no time to remedy it, and so you sometimes find these organizations simply going out of business because they haven't thought early enough about what they were doing" (Forrester, 1999)

The challenge as indicated by Jay Forrester is thus one of application, of finding the correct moment when the users of the models and their results are most receptive to them. This receptivity to the model and the utility of the model are according to Forrester, not in synchrony.

Regarding the method itself, it has been described as intellectually demanding, and requires the involvement of the end users, particularly when it reveals counterintuitive insights (Keough et al., 1992). A result of this, is that its application is intimately linked to group model building (Vennix, 1996).

7.8 Summary of the chapter

This chapter presented an analysis of the results that had been described in chapters 4, 5 and 6, the research questions were answered and implications to industry and academia are described from these results. The chapter ended by describing limitations of the research methods used in this thesis.

8 Summary of contributions

This chapter describes the contributions that have been presented throughout this thesis. To facilitate the presentation, the contributions have been categorized in two qualitative dimensions, 1) according to a strategic–operative spectrum and 2) according to an academia–industry spectrum. Beyond the content of the contributions themselves, the placements of these along the two dimensions is the subjective appreciation of the author, and reveal the relative placement of these contributions to each other rather than any absolute placement within these scales.

An *academic contribution* is related to advancement or implications to a research method or theory, while industrial contribution is related to advancement or implications to an operative method. A measure of this spectrum is the answer to a question such as "*how relevant or applicable is this contribution to an active company?*" The stronger the positive answer, the further towards the "industrial" end in the spectrum that the contribution is placed.

A *strategic contribution* is related to "*plans towards a goal*" in the long-term by a higher hierarchical level in the organization (Merriam-Webster, 2017) while the operational contribution is directed towards actions in the short term by a lower hierarchical

level in the organization. A measure of this spectrum is the answer to a question such as "*How high a hierarchical level is responsible for deciding on this contribution?*" The higher the required hierarchy, the further towards "strategy" end in the spectrum that the contribution is placed.

Figure 98 represents these two dimensions as a two by two matrix, laying out the different contributions within this matrix, contributions that are discussed next.

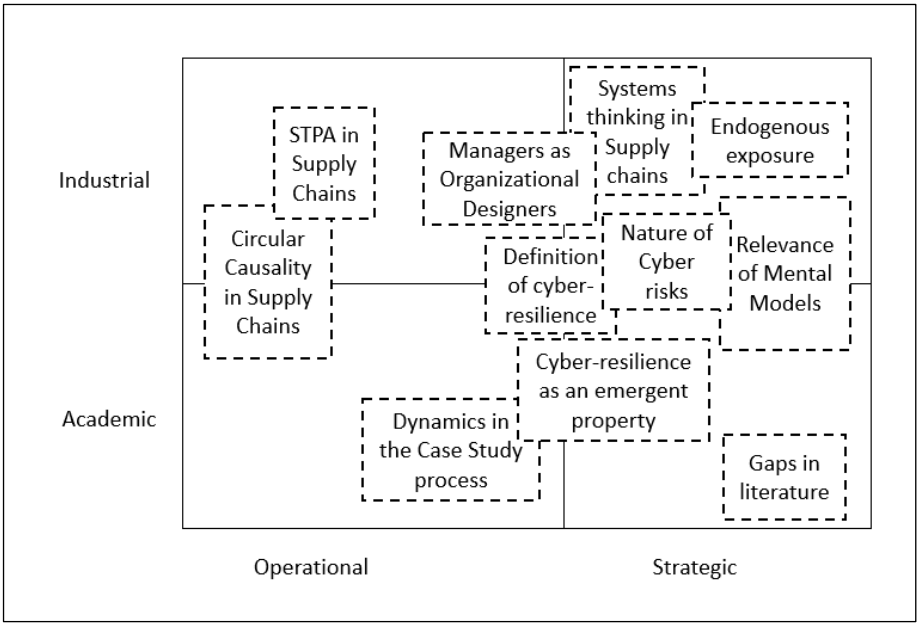

Figure 98 Thesis contributions and categories

8.1 The nature of cyber-risks to the supply chain

The archival and documental research uncovered different ways in which operations are disrupted when a cyber-risk materializes. Even though the analysis was not exhaustive, as the research strategy did not aim for one, the analysis to identify categories is nevertheless a contribution since:

- The analysis *provides a framework* of disruption mechanism classes that serves as a way of understanding new attacks, and which can be updated by new cyber-risk-related operational disruption types (see section 4.2).
- The analysis provides *relevant differences* with other supply chain risk types, and thus lays a justification towards the use of systemic risks and simulation analyses for managing these particular types of risks (see section 7.1.1)
- The analysis describes *different structures* through which cyber-attacks take place, providing base information for modelling and simulation of these cyber-attacks to explore reaction types (see section 4.2).
- The analysis describes the *differences between cyber-risks and other risks* in the supply chain, information needed as justification for the need of complementary methods for

cyber-risk management both in academic and industrial communities of interest (see section 7.1.2).

Cyber-attacks, by making unauthorized use of existing organizational infrastructure highlight that companies are exposed by omission, i.e., what companies have failed to do, at least to a similar degree as from commission, i.e., what has been done.

The examples seem to show that no matter how many walls continue to be built around organizations for protection against cyber-risks, this effort is defeated by the growth in complexity of connections between members of the system and with the environment.

8.2 Definition of cyber-resilience

The literature research gathered multiple definitions of cyber-resilience, through an analysis, a synthesis definition was proposed (See section 2.7.1):

"The capability of a system to minimize the effects on expected performance of a disruption caused by the manifestation of a cyber-risk"

This definition is a concise description of the characteristics of cyber-resilience

- It is a capability, which denotes the potential of reaching a condition, and it is thus an emergent property (see section 6.5),
- It has a focus on the expected performance, and as such, disruption is defined from the expectations,
- It is a counteraction to the manifestation of a cyber-risk

8.3 Gaps in extant literature about cyber-resilience

As a result of the systematic literature review, this thesis described gaps in the literature regarding cyber risks (see section 2.9). The structure proposed consisted in gaps along three categories, 1) The thing being managed, 2) the methods used to manage 3) and the people using the methods of management. This list of gaps and resulting research questions is shown in

Table 14. This categorization provides a research agenda for this domain, part of which is advanced through this thesis work.

8.4 Systems thinking for managing cyber-risks

In the search for effective tools to manage the response to unexpected events, academia in collaboration with industrial partners have developed a rich body of risk management frameworks during the past four decades and resilience frameworks for the last two decades. However, given the particular nature of cyber-risks, and the developing characteristics of the attacks against information networks with operational consequences, traditional risk analysis techniques appear to be ill-suited for the challenges presented by cyber-risks in complex supply networks. By focusing on the expected resulting behaviours and pre-existing capacities required for a resilient response, traditional frameworks comparatively overlook the capabilities required to activate, drive and control the response.

This work proposes a representation of circular causality for understanding both the exposure of supply chains to disruption of operations, and the development over time of the response to disruptions in the supply chain.

This contrasts directly with the mainstream approaches of representing disruption exposure and reaction as a linear process.

Paulsson et al. (2011) still considered linear approaches to understanding reaction, as seen in Figure 99.

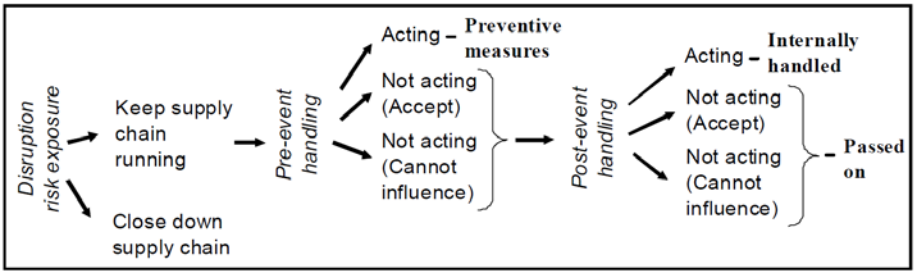

Figure 99 Disruption risk exposure (Paulsson et al., 2011)

Cross-disciplinary approach to resilience and the need for System Dynamics specialists. The information flow structures represented as a result of the SD model require a cross-disciplinary focus in an organization. This is an evidence of an organization-wide approach when understanding and designing an organization for resilient response.

A dynamic focus for designing a resilient response is an iterative, arduous process. If anyone expected to find a "formula" for understanding the dynamics in an organization, they might have been disappointed. The representation of the dynamics in the behaviours of an organization requires the understanding and application practice in concepts such as circular causality, stocks and flows, polarity and feedback loop types. Despite these concepts being easily related to experience once introduced, their application to a model is a process which has a steep learning

curve. The work here presented is aimed at laying a basic structure for understanding resilience, and future work will progress in the inclusion of long term structures that lead to a resilient response, and that are generalizable.

8.4.1 Systems thinking for supply chains

The STPA process, developed from the work by prof. Nancy Leveson (2011), despite having had applications in complex systems regarding production processes or had not been applied to the case of supply chains.

The process developed in this thesis, particularly the results shown in chapters 5 and 0, are a contribution to supply chain management by:

- Identifying a system structure of controllers, control actions, (See section 3.8.2)
- Identifying sources of risk in the structure (see section 5.2)
- Identifying levels of hierarchy (see section 5.2 and 6.5)
- Identifying levels of aggregation, resulting in the understanding of resilience as an emergent property only at certain levels of aggregation (see section 6.5)

8.4.2 Endogenous exposure

By considering "*exposure*" as a system state of "*having no protection from a financial loss*" (Merriam-Webster, 2017), endogenous exposure is the understanding of the sources of exposure as resulting from the structure that exists in the system, instead of looking for these disruptions from outside sources.

For the preparation phase, the endogenous exposure was described through the application of the systemic risk analysis method. The endogenous exposure was proposed as a measure of risk as derived from the current design of the supply chain, through the mapping of system structure and the identification of conditions that led the system to behave in an unwanted manner through the established control actions designed into this system. These "*Unsafe Control Actions*" reflected how the existing system structure could lead to an unwanted event irrespective of the trigger, as the analysis would be unchanged whether the trigger is from an internal or an external source, and whether the trigger is premeditated or accidental.

This approach changes the exogenous focus of analysis in some fundamental ways, as with an endogenous approach:

- The threat is not considered from outside the system but from within its own structure,

- Intentionality is not a relevant factor of analysis,
- The objective of the process is no longer system protection, rather system design, and
- Historical information is not fundamental for the analysis of endogenous exposure, a crucial advantage when dealing with situations for which historical information is restricted or non-existent.

The differences between an exogenous and endogenous approach to risk, is summarized in Table 40.

Table 40 Exogenous vs. endogenous risk assessment

Aspect	**Exogenous approach**	**Endogenous approach**
Source of risk	Outside the boundaries of the system.	Inside the boundaries of the system
Method of analysis	Rank the risk from external sources and protect system from external sources	Rank unsafe control actions and design the system for better response.
Risk Ranking	Probability and Severity	Number of Unsafe Control Actions
Relevance of Intentionality	Relevant for calculations of probability	Not relevant.
Relevance of past events / Need for historical evidence	Past events essential to determine probabilities of future events / Historical evidence is fundamental	Past events may point out undetected unsafe control actions to calculate relative probabilities (Historical evidence is not necessary)
Objective	System protection	System design

8.5 Dynamic simulation of cyber-risks

As foreseen by Jay Forrester as early as 1965 (Forrester, 1965), the activity of managers in an organization is related to design rather than to operation. However, "*lacking a systemic vision of causality [managers] have no way of knowing why policies often produce results directly opposite to those intended. But we do know this happens – all the time*" (Keough et al., 1992). The work presented in this thesis contributes directly to improving this lack of understanding. By testing systemic tools to uncover and structure systemic causalities behind the response to cyber-risks, it is expected that management will both increase activities towards the identification and understanding of these structures, and as a result will intensify the creation for ways in which these structures can be better designed for the objectives of the organization.

Additionally, the dynamics are part of the information contained in the members of the system. The models that members of an organization have about how this organization works, conditions how this organization is run: "*if men define situations*

as real, they are real in their consequences[31]" (Thomas et al., 1928). Additionally, "*people tend to look or information which confirms their viewpoint rather than to look for evidence that might refute it*" (Hogharth, 1987). Therefore the relevance of an explicit representation of those mental models for consensus, analysis and improvement cannot be overstated. The methods used in this thesis present the implementation of a way for representing these mental models.

8.6 Cyber-resilience as an emergent property

Resilience in general, and cyber-resilience in particular, through the dynamic model and its hierarchical structure representation, are understood as emergent properties (see section 3.2.1), as understood from a specific hierarchical level where this emergent property makes sense. Yet, the dynamic model presented in this thesis shows the need to understand the underlying structures that result in this resilience. However, the measurement of the resilience according to published methods

[31] This is known as the "Thomas Theorem".

does not point to ways in which to identify particular resilience values that are more convenient for an organization. Shorter and shallower consequences are better, but between shorter or shallower, no clear distinction can be made.

If cyber-resilience is understood as an emergent property, i.e., it is the result of multiple behaviours that are collectively understood from a specific hierarchical level, then "*too much*" or "*too little*" resilience loses meaning. Shape is an emergent property for example. In this case "*too much shape*" is not a sensible description. Rather, the discussion requires a different paradigm, of identifying the shape (in this case the cyber-resilience) needed for a particular objective.

8.7 Dynamic analysis in the case study process

As was discussed in section 7.6.2, the "dynamics" that is to be considered for the analysis of the evolution of a system's response over time is far more than what is currently understood as "dynamics" within the case study research method. This partial understanding of the "*dynamics*" concept in the case study method results in important data being overlooked during the research information gathering process. This information, suitable for modelling structure and simulating behaviour, has the potential of expanding the descriptive and exploratory nature of the traditional

case study (Yin, 1994) to applications into the structured-explanatory and evaluative-predictive applications.

The use of systems thinking during data gathering and analysis for a case study research, as presented in this thesis is an example of this approach, and illustrates the application of a system dynamics strategy for structuring and conducting the interview, for analysing the data, and for comparison between cases.

8.8 Contribution to theory and theory development

According to Boer et al. (2015), the development of a new theory is difficult and therefore "*research in management disciplines tends towards contributing to existing theory, or using existing theory to explain phenomena, rather than developing new theory*". The approach that has been taken in this thesis, based on Systems Thinking and through the use of the System Dynamics method, takes the traditional approach started by Jay Forrester, of building the theory about a phenomenon, from the observable world. Therefore, despite not presenting a contribution to the theory behind the methods used in this thesis, there are several contributions respect to the theory of the phenomena that this thesis is describing. This process is more in tune to the process suggested by Schemenner (Boer et al., 2015) of "discovery" rather than prematurely advancing one theory or another. Five relevant

contributions to theory and theory development derived from this work are mentioned next.

First, the systemic risk analysis in section 5 defines mechanisms that contribute to an accident, in this case, a cyber-event that requires a resilient response from the organization. This proposal is based on the implicit knowledge of the members in the organization, and can be potentially improved in future research efforts to cumulatively obtain a sound theory for the occurrence of cyber-attacks in organizations. This is a new contribution, as the literature review presented in this thesis did not reveal the proposal of such mechanisms involved in cyber-attacks in organizations. Theory development will follow as more such examples are analysed. A concept that is derived from this process is the endogenous exposure concept, and a method that results from this process when considering the concept of endogenous exposure, is the calculation of endogenous exposure.

Second, and in the same way as in the systemic risk analysis, system dynamics modelling provides, based on field data, a structure that leads to an observed behaviour, and as such is a contribution to theory development about structures that result in a resilient behaviour to cyber-events, similar to those presented by Fink et al. (2014) in its capacity for quantification, but more similar to the model by Tran et al. (2016), as the resilient response

is the complete result of the structure present in the system. As such, the results of this part of the research support the view that an endogenous explanation for the cyber-resilient behaviour is a plausible theory for describing the phenomenon of cyber-resilience, and that it can eventually lead to the prescriptive application of modelling towards these events.

Third, this thesis gathered descriptive data, again in the process of "discovery" related to the nature of cyber risks, was analysed in this thesis. This analysis performed in this thesis from that information, related to how cyber risks differ from other supply chain risks, is a contribution to theory development regarding cyber risks in supply chains, particularly with respect to their effect in the organization response to cyber-events.

Fourth, the thesis identifies shortcomings in the case study method with respect to the gathering of information over time, of the case's dynamics. This shortcoming is inherent in the definitions that are used for the case study. For example, Saunders et al. (2016) indicates that the case study "*the case study research sets out to study the dynamics of the topic being studied*", with these dynamics understood as "*the interactions between the subject of the case and its context*". This is a very restricted and vague definition, as there are dynamics inside the subject of study (if this subject was, say, a supply chain). This vague definition

does not consider other authors who have defined the dynamics in systems very precisely, as consisting of accumulations, circular causality in the form of feedback loops and resulting meta-structures such as delays. It is therefore plausible that the current definition of a case study will leave useful information in the field. An expanded definition of a case study should consider specific, generic structures that can be identified by the actors of the system or subject of the study.

Finally, the thesis proposes a new theory of resilience from the scope of cyber-resilience. This theory has the starting point in the "endogenous nature of cyber risks" and defines the cyber risks as a consequence of structures existing in the organization that allow a cyber-event. These structures, akin to an open door in a building we want to keep inaccessible, can lead to cyber events that need a resilient response, both from external or internal agents. In fact, from the point of view of this endogenous theory, the source of the attacks is irrelevant.

8.9 Summary of chapter

This chapter described the contributions that had been presented throughout this thesis. A categorization was proposed for these contributions, and these were described in detail.

9 Conclusions and potential research

This chapter presents the conclusion of this work by making an overview of the thesis process, and the context from which the problem statement was proposed, the methods used and the conclusions that were reached. The chapter ends by proposing areas of further research derived from this work.

9.1 Conclusion

The overall objective of this thesis was the derivation of tools for the improved management of cyber-risks in supply chains (see Table 1 for a list of the objectives). The tools used in this thesis were derived starting from a scientific analysis of the current state of knowledge about the topic domain, and of empirical data about cyber-risks. A structure of enquiry was followed by initially understanding the distinctive nature of cyber-risks with respect to other supply chain risks, and finally by developing tools that address some of these gaps.

The findings of the research are in three main domains. First, the research reveals relevant gaps in the traditional methods available for the management of cyber risks, as these do not consider behaviour over time (dynamic behaviour), rely on inadequate or difficult reporting of events, depend on historical data to manage unknown or new attacks, and adopt a silo-

approach for managing a problem that is cross-disciplinary. Second, the analysis finds differences between cyber-risks and other supply chain risks, such as the capacity of disruptions from cyber risks to go undetected, the high reproduction fidelity of cyber-risks, the capacity of cyber risks to affect different geographical locations simultaneously, or the complexity of cyber-attacks. Finally, the research reveals that the novel use of methods based in systems thinking for managing cyber-risks simultaneously address gaps found in traditional methods, and provide a foundation for thinking about cyber-risks not as an outside threat, but rather created by the supply chain itself, as the result of incomplete requirements to the supply chain design.

The implications for practitioners suggest that supply chains can design the behaviours they require through cross-disciplinary, simulation-based techniques, and that modularity helps to manage complexity. The implications for academics suggest that reporting methods regarding cyber-attacks have to be adjusted to match the quick development of these threats, a cross-disciplinary cyber-risk and resilience research community needs to be identified and fostered, and current research methods need to be expanded to integrate dynamic systems thinking into the data gathering and analysis.

From the understanding that supply chains are a network of processes for the production and distribution of goods and services, based on underlying information flows and storage, this thesis claimed as a contribution that an “endogenous” approach of causality for understanding cyber-risks results in actionable insights independent of the source of threat to operations.

This work argues that despite the relevant advances that have been made in regard to Information Technology (IT) in organizations (both towards enabling systems to communicate and store data, and to allow collaboration more accurately) and of risk management towards IT and supply chain management (SCM), these are misdirected due to the particular nature of the threat presented by cyber-attacks, problem that is to a large extent one of social decisions and organizational design towards timely and effective reaction (cyber-resilience) that actively involves other areas of the organization beyond only IT management.

Traditional approaches for solutions to cyber-risks rely predominantly on IT, expecting to build walls around the organization to make access more difficult for attackers. These are incomplete at best and misguided at worst, as they do not explore the actual causes that are leading to the breaches, by pursuing and temporarily solving only the symptoms. In this way, organizations not only enable and provide incentives for an ever-increasing

stream of defence artefacts that decrease organizational flexibility and increase dependence on IT-consultants, but also perpetuate the real underlying problem that lies behind the unwanted behaviour i.e., cyber-attacks, and which relates to the existing structures that make these attacks possible.

By sequentially answering the main research question, this work derives the proposal of systems-thinking-based approaches to understanding and managing cyber-risks. These approaches are characterized by considering the supply chain's own structure and not outside forces, as the main focus when understanding an unwanted behaviour such as the disruption from a cyber-attack. A systems thinking approach is the philosophical pivot point that justifies a change in focus from protecting systems against outside threats to understanding the reactions of systems according to their structure, changed focus that will increase the likelihood of a supply chains reacting as intended and recovering swiftly to whatever disruption materializes.

9.2 Potential research

Several avenues of further research are opened through the results presented in this work. Some of these are discussed next.

9.2.1 Exploration of other data gathering processes

The process chosen for researching the nature of cyber-risks in their effects towards operational disruption was through an archival and documentary research process. Other possibilities can be explored, for example:

- Forming strategic alliances with companies or industrial unions, to obtain direct information when a cyber-attack has been detected to gather primary data as contingency plans are implemented by the company under attack. However, before this is possible, 1) companies have to be willing to share data, often sensitive data while an attack is happening, and 2) companies have to understand the role of resilience design and management engineering, beyond an IT response, as the strategic option to take.
- Producing a survey to be answered by companies about the cyber-attacks they have experienced. However, 1) as was seen in the methodology section, a survey can deliver historical information that is limited or inexistent in the case of cyber-risks. As a result this is not an indication of any sort about the attacks that could be experienced in future, and 2) surveys have to be complemented by directed interviews considering a dynamic framework, to gather data

that is useful in the management of organizational response to cyber-risks.

9.2.2 Improvement of the models

The models that were considered for the research have assumptions and simplifications which limit their applicability and thus offer an opportunity for further research.

For the case of the systemic risk analysis, despite the risk analysis model having followed a clear process, the level of aggregation is a choice in the analysis that can be improved. For example:

- The chosen controllers respond to a first level of analysis that can be improved to consider, for example, the inner structure of the plant, finance procurement and warehousing as explicit controllers, and the understanding of how communication design can be improved. It is always possible to go to increasing levels of detail when dealing with human action, yet it has been found that modelling human behaviour in detail is difficult to achieve (Leveson, 2011). As a result some level of aggregation has been the norm when modelling.
- Use of CAST for analysis of past attack events can potentially reveal information about the sensibility of

existing supply chain structures, for the prioritization of improvement actions.

For the case of the system dynamics model, the model that was developed for this thesis, is an approximation that can benefit from a series of improvements, such as

- The calculation of customer base
- The performance decision algorithm. Despite the case having an attack indication signal declared through the exogenous information delivered by the federal agency that told ABC industries of an attack taking place, this needs not be so. Technologies such as Artificial Intelligence (AI) are gaining ground as tools for continuous condition monitoring and discrimination of states that are unusual or likely to lead to a disruption. Therefore a place for improvement is through the consideration of alternate algorithms within the performance tracker, to identify ranges of operation where these might make sense, and situations where these are most effective.

9.2.3 Systems analysis education in management

The models presented and developed in this work, despite diverse simplifications and assumptions during their creation and analysis, evidence the ever increasing complex nature of the

organizations that need to be designed and managed. Additionally the dynamic way in which the systems are studied in this work (i.e., these evolve over time) has shown that this behaviour can quickly exceed any understanding that can be provided by intuition alone.

Models have shown their contribution in different aspects, from providing a method to structure the mental models present in the members of the organization, to proposing an explicit way of representing these mental models for collaboration and alignment. However, the gap between the usefulness of these tools and the perception by management is considerable.

Different authors have put forward reasons why this is as come to be the case. Alleged reasons include for example the difficulty for management to focus on medium to long term simulation while at the same time having short term objectives and operational pressure; the non-linear nature of the system modelling process with a steep learning curve.

The communication to companies about the usefulness of understanding the dynamic nature of the organizations that need to be managed, is unsurprisingly a slow one, to which this work expects to contribute, but which needs an available knowledge base both among managers and among researchers. For this, it is

proposed that the education of dynamics, and particularly system dynamic modelling and simulation be included in the basic management engineering education curriculum. This has been advanced by universities around the world such as the Massachusetts Institute of Technology, Delft University of Technology, the University of Bergen, the University of Manchester, the National University of Singapore, and Stellenbosch University in South Africa.

9.2.4 Cyber-risk from a management perspective.

The research that was carried out in this thesis explored the concept of cyber-risks beyond its technical implications, and as the literature review clearly showed, the problem of cyber-risks is one that is more about collaboration and organizational design that about protection and merely information safeguarding.

This work is expected to serve as a stepping stone towards further research into the relevance of management engineering, of the design of the organization that are being created, into the effective prevention and response of risks such as cyber-risks.

9.2.5 Incentives in cyber-risk information sharing

The research in both the systematic literature review and the archival research evidenced a lack of information about cyber-

risks as derived from cyber-attacks to supply chains. This restricted information access, an organizational behaviour, according the systems thinking framework is the result of an underlying structure. Evidence about the damaging market effects of a cyber-attack disclosure on the company that is making the disclosure, points towards strong incentives to limit or delay disclosure. The exploration of these incentive structure, and how it can be influenced or changed for more effective data sharing is an area open for research.

10 References

Abdulkhaleq, A. and Wagner, S., 2015. XSTAMPP: an eXtensible STAMP platform as tool support for safety engineering. 2015 STAMP Conference, MIT, Boston, 2015

Asbjornslett, B.E. and Rausand, M., 1999. Assess the vulnerability of your production system. *Production Planning and Control*, 10(3), pp.219-229.

Ahmad, A., Johnson, C. and Storer, T., 2015. An Investigation on Organisation Cyber-resilience. World Academy of Science, Engineering and Technology, *International Journal of Computer, Electrical, Automation, Control and Information Engineering*, 9(7), pp.1703-1708.

Allen, K. 2014. *Hackers blackmail Sony Pictures, attack computer network.* [online] CNBC online edition. Available at: http://www.cnbc.com/id/102216690 [Accessed 31 May 2016]

Andersen, D.F., Richardson, G.P. and Vennix, J.A., 1997. *Group model building: adding more science to the craft*. Wiley and Sons.

Anderson, R., 1993, December. Why cryptosystems fail. In *Proceedings of the 1st ACM Conference on Computer and Communications Security* (pp. 215-227). ACM.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M.J., Levi, M., Moore, T. and Savage, S., 2013. *Measuring the cost of cybercrime. In The economics of information security and privacy* . Springer Berlin Heidelberg. pp. 265-300.

Andrijcic, E. and Horowitz, B., 2006. A Macro-Economic Framework for Evaluation of Cyber Security Risks Related to Protection of Intellectual Property. *Risk analysis*, 26(4), pp.907-923.

Annas, J., 1981. *An introduction to Plato's Republic*. Oxford University Press.

APICS, American Production and Inventory Control Society, Council, S.C., 2010. *Supply-chain operations reference-model*. Overview of SCOR version 10.

Arghandeh, R., von Meier, A., Mehrmanesh, L. and Mili, L., 2016. On the definition of cyber-physical resilience in power systems. *Renewable and Sustainable Energy Reviews*, 58, pp.1060-1069.

Arnold, R.D. and Wade, J.P., 2015. A definition of systems thinking: a systems approach. *Procedia Computer Science*, 44, pp.669-678.

Asbjornslett, B. E. 1999. Assess the vulnerability of your production system. *Production Planning & Control*, 10(3): 219–229.

Asbjornslett, B. E., Rausland, M., 1999. Assess the vulnerability of your production system. *Production Planning & Control*, 10(3): 219–229.

Ashok, A., Govindarasu, M. and Wang, J., 2017. Cyber-Physical Attack-Resilient Wide-Area Monitoring, Protection, and Control for the Power Grid. *Proceedings of the IEEE*.

Axelrod, R.M., 1997. *The complexity of cooperation: Agent-based models of competition and collaboration*. Princeton University Press.

Bailey, T., Miglio, A. Del, & Richter, W. 2014. The rising strategic risks of cyberattacks. *McKinsey Quarterly*. May 2014.

Banos, V., Kim, Y., Ross, S. and Manolopoulos, Y., 2013. CLEAR: a credible method to evaluate website archivability. In: *International Conference on Preservation of Digital Objects (iPRES 2013)*, Lisbon, Portugal, 2-6 Sep 2013.

Barlas, Y., 1996. Formal aspects of model validity and validation in system dynamics. *System dynamics review*, 12(3), pp.183-210.

Barron, S., Cho, Y.M., Hua, A., Norcross, W., Voigt, J. and Haimes, Y., 2016, April. Systems-based cyber security in the

supply chain. In: *Systems and Information Engineering Design Symposium (SIEDS)*, 2016 IEEE (pp. 20-25). IEEE.

Bartlett, J., 2015. *The dark net: Inside the digital underworld*. Melville House.

Bayuk, J. L., Healey, J., Rohmeyer, P., Sachs, M. H., Schmidt, J., & Weiss, Jj. (2012). *Cyber security policy guidebook*. John Wiley and Sons.

BBC, 2017. *Global ransomware attack causes turmoil*. [online] BBC News 28 June 2017. Available at: http://www.bbc.com/news/technology-40416611 [Acessed 15 Jun. 2017]

Bekkers, R., Duysters, G. and Verspagen, B., 2002. Intellectual property rights, strategic technology agreements and market structure: The case of GSM. *Research Policy*, 31(7), pp.1141-1161.

Bennett, S.A., 2016. The benefits of a systems-thinking approach to accident investigation. In: *Applications of Systems Thinking and Soft Operations Research in Managing Complexity*. Springer International Publishing. pp. 203-226.

Besiou, M., Stapleton, O. and Van Wassenhove, L.N., 2011. System dynamics for humanitarian operations. *Journal of Humanitarian Logistics and Supply Chain Management*, 1(1), pp.78-103.

Björck, F., Henkel, M., Stirna, J. and Zdravkovic, J., 2015, March. Cyber-resilience-Fundamentals for a Definition. In *WorldCIST (1)* (pp. 311-316).

Blackhurst, J., Dunn, K. S., & Craighead, C. W. 2011. An Empirically Derived Framework of Global Supply Resiliency. *Journal of Business Logistics*, 32(4): 374–391.

Blakeslee, S., 2004. The CRAAP test. *LOEX Quarterly*, 31(3), p.4.

Boell, S.K. and Cecez-Kecmanovic, D., 2014. A hermeneutic approach for conducting literature reviews and literature searches. *CAIS*, 34, p.12.

Boer, H., Holweg, M., Kilduff, M., Pagell, M., Schmenner, R. and Voss, C., 2015. Making a meaningful contribution to theory. *International Journal of Operations & Production Management*, 35(9), pp.1231-1252.

Booth, W.C., Colomb, G.G. and Williams, J.M., 2008. *The craft of research*. 3rd edition, University of Chicago press.

Bossel, H., 1994. *Modelling and Simulation*, A.K. Pieters & Verwieg Verlag, Welesley, MA, USA.

Bosworth, D. and Rogers, M., 2001. Market value, R&D and intellectual property: an empirical analysis of large Australian firms. *Economic Record*, 77(239), pp.323-337.

Boyes, H., 2015. Cybersecurity and cyber-resilient supply chains. *Technology Innovation Management Review*, 5(4), p.28.

Boyson, S., 2014. Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. *Technovation*, 34(7), pp.342-353.

Bradley, T. Security experts weigh in on Wikileaks "Vault 7" dump. Forbes Cyber-security Newsletter, accessed on 10 April 2017, https://www.forbes.com/sites/tonybradley/2017/03/07/security-experts-weigh-in-on-wikileaks-vault-7-dump/#8eda98c1690e

Brereton, P., Kitchenham, B.A., Budgen, D., Turner, M. and Khalil, M., 2007. Lessons from applying the systematic literature review process within the software engineering domain. Journal of systems and software, 80(4), pp.571-583.

Brown, H.S., 2016. After the data breach: Managing the crisis and mitigating the impact. Journal of business continuity & emergency planning, 9(4), pp.317-328.

Buchwald, J.Z. ed., 1996. Scientific credibility and technical standards in 19th and early 20th century Germany and Britain (Vol. 1). Springer Science & Business Media.

Burnson, P. 2013. Supply chain cybersecurity: a team effort. Supply Chain Management Review, (June): 6–8.

Bush, G. W. 2003. The national strategy to secure cyberspace.
Carroll, J.S., 1998. Organizational learning activities in high-hazard industries: the logics underlying self-analysis. Journal of Management studies, 35(6), pp.699-717.
Cashell, B., Jackson, W.D., Jickling, M. and Webel, B., 2004. The economic impact of cyber-attacks. Congressional Research Service Documents, CRS RL32331 (Washington DC).
Chappell, B., Penman, M. Ransomware attacks ravage computer networks in dozen of countries. National Public Radio, NPR International website, accessed on 10 August 2017, http://www.npr.org/sections/thetwo-way/2017/05/12/528119808/large-cyber-attack-hits-englands-nhs-hospital-system-ransoms-demanded
Charmaz, K., 2014. Constructing grounded theory. Sage.
Chase, S.E., 2011. Narrative inquiry: Still a field in the making. The Sage handbook of qualitative research, 4, pp.421-434.
Checkland, P., 1981. Systems thinking, systems practice. John Wiley & Sons, New York.
Christopher, M., 2011. Logistics & supply chain management. Pearson UK.
Christopher, M., & Peck, H. 2004. Building the Resilient Supply Chain. International Journal of Logistics Management, 15(2): 1–14.
Christopher, M., & Towill, D. 2001. An integrated model for the design of agile supply chains. International Journal of Physical Distribution & Logistics Management, 31(4): 235–246.
Christopher, M., Peck, H., Abley, J., Haywood, M., Saw, R., Rutherford, C., & Strathern, M. (2003). Supply Chain Resilience.
Cisco, 2017. Annual Cybersecurity Report 2017. Cisco online website. Accessed 01 August 2017. http://b2me.cisco.com/en-us-annual-cybersecurity-report-2017

Clarke, M. and Oxman, A.D., 2004. Cochrane Reviewers Handbook 4.2.1 [updated March 2004]; The Cochrane Library.

Clinton, B. 1998. Presidential Decision Directive/ NSC-63 on Critical Infrastructure protection. Department of State Official presidential directive. http://www.fas.org/irp/offdocs/pdd/pdd-63.htm.

Coghlan, D. and Brannick, T., 2014. Doing action research in your own organization. Sage.

Cohen, J., 1960. A coefficient of agreement for nominal scales. Educational and psychological measurement, 20(1), pp.37-46.

Cohen, K.J. and Cyert, R.M., 1965. Simulation of organizational behaviour. Handbook of organizations, pp.305-334.

Collier, Z.A., Linkov, I. and Lambert, J.H., 2013. Four domains of cybersecurity: a risk-based systems approach to cyber decisions. Environment Systems and Decisions, 4(33), pp.469-470.

Conklin, W.A., Shoemaker, D. and Kohnke, A., 2017. Cyber-resilience: Rethinking Cybersecurity Strategy to Build a Cyber Resilient Architecture. In ICMLG2017 5th International Conference on Management Leadership and Governance (p. 105). Academic Conferences and publishing limited.

Cooper, H.M., Patall, E.A. and Lindsay, J.J., 2008. Research synthesis and meta-analysis. The Sage handbook of applied social research methods.

Cooper, K.G., 1980. Naval ship production: A claim settled and a framework built. Interfaces, 10(6), pp.20-36.

Cutter, S.L., Ahearn, J.A., Amadei, B., Crawford, P., Eide, E.A., Galloway, G.E., Goodchild, M.F., Kunreuther, H.C., Li-Vollmer, M., Schoch-Spana, M. and Scrimshaw, S.C., 2013. Disaster resilience: A national imperative.

Environment: Science and Policy for Sustainable Development, 55(2), pp.25-29.

Da Xu, L., He, W. and Li, S., 2014. Internet of things in industries: A survey. IEEE Transactions on industrial informatics, 10(4), pp.2233-2243.

Daniels, C.E., Montori, V.M. and Dupras, D.M., 2002. Effect of publication bias on retrieval bias. Academic Medicine, 77(3), p.266.

Davis, A., 2015. Building cyber-resilience into supply chains. Technology Innovation Management Review, 5(4), p.19.

de Crespigny, M., 2012. Building cyber-resilience to tackle threats. Network Security, 2012(4), pp.5-8.

Dederick, J., Xin Xu, S., Xiaoguo, K. Z., 2008, "How does information technology shape supply-chain structure? Evidence on the number of suppliers", Journal of Management Information Systems, 25(2), p. 41-72.

Deloitte. 2012. Aftershock - Adjusting to the new world of risk management Contents.

Deloitte. 2013. The ripple effect - How manufacturing and retail executives view the growing challenge of supply chain risk.

Denyer, D. and Tranfield, D., 2009. Producing a systematic review. The Sage handbook of applied social research methods, p. 671-689.

DHL, 2015. Resilience360 – Managing risks in your supply chain. DHL Website: https://resilience360.com/ [Accessed on 21 August, 2017]

DiMase, D., Collier, Z.A., Heffner, K. and Linkov, I., 2015. Systems engineering framework for cyber physical security and resilience. Environment Systems and Decisions, 35(2), pp.291-300.

Drost, E.A., 2011. Validity and reliability in social science research. *Education Research and perspectives*, 38(1), p.105.

Durach, C.F., Kembro, J. and Wieland, A., 2017. A New Paradigm for Systematic Literature Reviews in Supply Chain Management. *Journal of Supply Chain Management*, 53(4), pp. 67-85.

Durden, T. Wikileaks unveils “vault 7”: the largest ever publication of confidential CIA documents; another Snowden emerges. Zerohedge News, Website accessed on 10 April 2017, http://www.zerohedge.com/news/2017-03-07/wikileaks-hold-press-conference-vault-7-release-8am-eastern

Earl, M.J., 1996. The risks of outsourcing IT. Sloan management review, 37(3), p.26.

Edmondson, G., Baker, S. 1997. Silicon Valley on the Rhine, Business Week, 3 November, pp. 40-47.

Eggert, L. and Hofmann, A., 2016. Managing supply chain disruption risks through insurance solutions: current practices and challenges. International Journal of Management and Decision Making, 15(2), pp.154-166.

Elazari, Keren. 2014. Hackers: the internet’s immune system. TED. Mar. 2014. Lecture. Website accessed 01 March 2016, https://www.ted.com/talks/keren_elazari_hackers_the_internet_s_immune_system

Ellram, L. M., 1996. The use of the case study method in logistics research, Journal of Business logistics, 17(2): 93-137.

Emery, F. E., and E. L. Trist. 1960. "Socio-technical Systems." In Management Sciences Models and Techniques, vol. 2. London.

ENISA, 2012. Existing Taxonomies. ENISA Website: https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/existing-taxonomies [Accessed on 21 August, 2017]

Fanelli, D., 2011. Negative results are disappearing from most disciplines and countries. Scientometrics, 90(3), pp.891-904.

FBI, 2016. Internet crime report, FBI Internet crime compliant centre. Website: https://pdf.ic3.gov/2016_IC3Report.pdf, accessed 16 August 2017.

Felson, D.T., 1992. Bias in meta-analytic research. Journal of clinical epidemiology, 45(8), pp.885-892.

Ferdinand, J., 2015. Building organisational cyber-resilience: A strategic knowledge-based view of cyber security management. Journal of business continuity & emergency planning, 9(2), pp.185-195.

Fine, C., 1998. Clockspeed. Basic Books, Revised edition, USA.

Fink, G.A., Griswold, R.L. and Beech, Z.W., 2014, August. Quantifying cyber-resilience against resource-exhaustion attacks. In Resilient Control Systems (ISRCS), 2014 7th International Symposium on (pp. 1-8). IEEE.

Fleiss, J.L., 1971. Measuring nominal scale agreement among many raters. Psychological bulletin, 76(5), p.378.

Florêncio, D. and Herley, C., 2013. Sex, lies and cyber-crime surveys. In Economics of information security and privacy III (pp. 35-53). Springer, New York, NY.

Forrester, J.W, 1961. Industrial dynamics. System dynamics series, Pegasus Communications, Waltham, MA, USA.

Forrester, J.W., 1965. A new corporate design. IMR; Industrial Management Review (pre-1986), 7(1), p.5.

Forrester, J.W., 1999. The Forrester Seminar Series on System Dynamics. Session D: Non-Linearity. System Dynamics Society.

Foxx, C., 2017. NHS cyber-attack: GPs and hospitals hit by ransomware. BBC News. Accessed on 20 May 2017. http://www.bbc.com/news/health-39899646

Freimann, J., 1994. Das Theorie-Praxis-Dilemma der Betriebswirtschaftslehre. Fischer-Winkelmann, W.(Hg.): Das Theorie-Praxis-Problem der Betriebswirtschaftslehre, Wiesbaden, pp.7-24.

Frosdick, M. (1997), “The techniques of risk management are insufficient in themselves”,Disaster Prevention and Management, Vol. 6 No. 3, pp. 165-77

Ghadge, A., Dani, S., 2013. A systems approach for modelling supply chain risks, Supply Chain Management: An international Journal, 18(5), pp. 523-538.

Gilbert, N. and Troitzsch, K., 2005. Simulation for the social scientist. McGraw-Hill Education (UK).

Gilbert, R.J. and Newbery, D.M., 1982. Pre-emptive patenting and the persist

Glaessner, T., Kellermann, T. and McNevin, V., 2002. Electronic security: Risk mitigation in financial transactions. Policy Working Paper, 2870.

Glaser, B.G., Strauss, A.L., 1967. The discovery of grounded theory. Chicago, Il, Aldine.

Glöser-Chahoud, S., Hartwig, J., Wheat, I.D. and Faulstich, M., 2016. The cobweb theorem and delays in adjusting supply in metals' markets. System Dynamics Review, 32(3-4), pp.279-308.

Goldman, H.G., 2010. Building secure, resilient architectures for cyber mission assurance. The MITRE Corporation.

Gonzalez, J.J. and Trcek, D., 2017, January. Proper Incentives for Proper IT Security Management–A System Dynamics Approach. In Proceedings of the 50th Hawaii International Conference on System Sciences.

Goodman, M., 2015. Future crimes: Everything is connected, everyone is vulnerable and what we can do about it. Anchor.

Granqvist, E., 2015. Why science needs to publish negative results. Elsevier Connect.

Grix, J., 2002. Introducing students to the generic terminology of social research. Politics, 22(3).

Gunasekaran, A., Subramanian, N. and Papadopoulos, T., 2017. Information technology for competitive advantage within logistics and supply chains: A review. Transportation

Research Part E: Logistics and Transportation Review, 99, pp.14-33.

Hansen, G.S. and Wernerfelt, B., 1989. Determinants of firm performance: The relative importance of economic and organizational factors. Strategic management journal, 10(5), pp.399-411.

Harrison, J.R., Lin, Z., Carroll, G.R. and Carley, K.M., 2007. Simulation modelling in organizational and management research. Academy of Management Review, 32(4), pp.1229-1245.

Hathaway, O.A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W. and Spiegel, J., 2012. The law of cyber-attack. California Law Review, pp.817-885.

Heron, J., 1996. Co-operative inquiry: Research into the human condition. Sage.

Herrington, L. and Aldrich, R., 2013. The future of cyber-resilience in an age of global complexity. Politics, 33(4), pp.299-310.

Hogarth, R., 1987. Judgement and Choice: The Psychology of Decision. Chichester, New York, Brisbane.

Homer, J., Ritchie-Dunham, J., Rabbino, H., Puente, L.M., Jorgensen, J. and Hendricks, K., 2000. Toward a dynamic theory of antibiotic resistance. System Dynamics Review, 16(4), pp.287-319.

Homer, J.B. and Hirsch, G.B., 2006. System dynamics modelling for public health: background and opportunities. American journal of public health, 96(3), pp.452-458.

Homer, J.B., 1985. Worker burnout: A dynamic model with implications for prevention and control. System Dynamics Review, 1(1), pp.42-62.

Hult, F., Sivanesan, G., 2014. Introducing cyber. Journal of business continuity & emergency planning, 7(2), pp.97-102.

Hyman, P., 2013. Cybercrime: it's serious, but exactly how serious? Communications of the ACM, 56(3), pp.18-20.

IBM, 2017. Bringing big data to the enterprise. Website accessed on 21 April 2017, https://www-01.ibm.com/software/data/bigdata/what-is-big-data.html

IC3, 2017, Federal Bureau of Investigation Internet Crime Complaint Centre (IC3) Website, Accessed on 02 July 2017: https://www.ic3.gov/faq/default.aspx

Jalili, Y. and Ford, D.N., 2016. Quantifying the impacts of rework, schedule pressure, and ripple effect loops on project schedule performance. System Dynamics Review, 32(1), pp.82-96.

James, L.R., Demaree, R.G. and Wolf, G., 1984. Estimating within-group interrater reliability with and without response bias. Journal of applied psychology, 69(1), p.85.

Jennex, M.E., 2015. Literature Reviews and the Review Process: An Editor-in-Chief's Perspective. Communications of the Association for Information Systems, 36.

Jesson, J., Matheson, L. and Lacey, F.M., 2011. Doing your literature review: Traditional and systematic techniques. Sage.

Jin, D., Li, Z., Hannon, C., Chen, C., Wang, J., Shahidehpour, M. and Lee, C.W., 2017. Towards a Cyber Resilient and Secure Microgrid Using Software-Defined Networking. IEEE Transactions on Smart Grid.

Johnson-Laird, P.N., 1983. Mental models. Cambridge University Press.

Kang, K. M., Jae, M, 2005. A quantitative assessment of LCOs for operations using system dynamics, Reliability Engineering and System Safety, 87, pp.211-222.

Kanwar, S. and Evenson, R., 2003. Does intellectual property protection spur technological change? Oxford Economic Papers, 55(2), pp.235-264.

Katz, J. (2013). Cyber Security Deterrence and IT Protection for Critical Infrastructures (p. 82). Springer. doi:10.1007/978-3-319-02279-6

Keegan, C. 2014. Cyber security in the supply chain: A perspective from the insurance industry. Technovation, 34(7): 380–381.

Keough, M. and Doman, A., 1992. The CEO as organization designer. The McKinsey Quarterly, (2), pp.3-31.

Khan, O. and Burnes, B., 2007. Risk and supply chain management: creating a research agenda. The international journal of logistics management, 18(2), pp.197-216.

Khan, O. and Estay, D.A.S., 2015a. Supply chain cyber-resilience: Creating an agenda for future research. Technology Innovation Management Review, 5(4).

Khan, Y.I., Al-Shaer, E. and Rauf, U., 2015b, October. Cyber-resilience-by-Construction: Modelling, Measuring & Verifying. In Proceedings of the 2015 Workshop on Automated Decision Making for Active Cyber Defence (pp. 9-14). ACM.

Kiechel, W., 2010. The lords of strategy: The secret intellectual history of the new corporate world. Harvard Business Press.

King, G., Keohane, R.O. and Verba, S., 1994. Designing social inquiry: Scientific inference in qualitative research. Princeton university press.

Kletz, T., 1988. Wise after the event. Control and Instrumentation, 20, p.57.

Kossovsky, N., Brandegee, B. and Giordan, J.C., 2004. Using the market to determine IP's fair market value. Research-Technology Management, 47(3), pp.33-42.

Kuhn, T.S., 1962. “The structure of scientific revolutions”. The University of Chicago Press, Chicago, USA.

Kushner, D. 2013. The real story of stuxnet. IEEE Spectrum online edition. http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

Kushner, D., 2013. The real story of Stuxnet. IEEE Spectrum, 3(50), pp.48-53.

Lemos, R., 2005. eBay pulls vulnerability auction, Security Focus news, website accessed on 21 April 2017, http://www.securityfocus.com/news/11363

Leveson, N., 1995. Safeware: System safety and computers.

Leveson, N., 2011. Engineering a safer world: Systems thinking applied to safety. Mit Press.

Leveson, N.G., 1995. Safeware. System Safety and Computers. Addison Wesley.

Levy, S., 2001. Hackers: Heroes of the computer revolution (Vol. 4). New York: Penguin Books.

Li, Z., Shahidehpour, M. and Aminifar, F., 2017. Cybersecurity in Distributed Power Systems. Proceedings of the IEEE.

Libert, B., Beck, M., Wind, J., 2016. The network imperative: how to survive and grow in the age of digital business models, Boston, Massachusetts: Harvard Business Review Press

Linkov, I., Eisenberg, D. A., Bates, M. E., Chang, D., Convertino, M. 2013a. Measurable resilience for actionable policy. *Environmental Science and Technology*, 47(ii): 10108–10110.

Linkov, I., Eisenberg, D. a., Plourde, K., Seager, T. P., Allen, J. 2013b. Resilience metrics for cyber systems. *Environment Systems and Decisions*, 33(4): 471–476.

Littell, J.H., Corcoran, J. and Pillai, V., 2008. Systematic reviews and meta-analysis. Oxford University Press.

Maersk. 2017. Interim report Q2 2017. Maersk online website. Accessed on 18 August 2017. http://files.shareholder.com/downloads/ABEA-3GG91Y/5069836763x0x954061/7EB88BAD-F1AE-4E86-9B95-FF32017D31F9/APMM_Interim_Report_Q2_2017.pdf

Mallett, R., Hagen-Zanker, J., Slater, R. and Duvendack, M., 2012. The benefits and challenges of using systematic reviews in international development research. Journal of development effectiveness, 4(3), pp.445-455.

Marks, P., 2011. Dot-dash-diss: The gentleman hacker's 1903 lulz. NewScientist2011.

Martinez-Moyano, I.J. and Richardson, G.P., 2013. Best practices in system dynamics modelling. System Dynamics Review, 29(2), pp.102-123.

Mass, N., 1980. Stock and flow variables and the dynamics of supply and demand, in Randers, J. ed., Elements of system dynamics method. Wright Allen Pr.

McAfee, 2014. Net Losses: Estimating the global cost of cybercrime; economic impact of cybercrime II, United States Center for Strategic and International Studies.

McCarthy, J.T., Hocum, C.L., Albright, R.C., Rogers, J., Gallaher, E.J., Steensma, D.P., Gudgell, S.F., Bergstralh, E.J., Dillon, J.C., Hickson, L.J. and Williams, A.W., 2014, January. Biomedical system dynamics to improve anemia control with darbepoetin alfa in long-term hemodialysis patients. In Mayo Clinic Proceedings (Vol. 89, No. 1, pp. 87-94). Elsevier.

McGowan, J. and Sampson, M., 2005. Systematic reviews need systematic searchers. Journal of the Medical Library Association, 93(1), p.74.

McQueen, M.A., Boyer, W.F., Flynn, M.A. and Beitel, G.A., 2006. Time-to-compromise model for cyber-risk reduction estimation. In Quality of Protection (pp. 49-64). Springer, Boston, MA.

Meadows, D.H., 1980. The unavoidable a priori. Elements of the system dynamics method. Productivity Press, Cambridge, MA, pp.23-57.

Meadows, D. and Robinson, J.M., 1985. The electronic oracle: computer models and social decisions. John Wiley & Sons.

Meadows, D.H., 2008. Thinking in systems: A primer. Chelsea green publishing.

Mendelson, H. and Pillai, R.R., 1998. Clockspeed and informational response: Evidence from the information

technology industry. Information Systems Research, 9(4), pp.415-433.

Merriam-Webster, 2017. Online dictionary. Accessed on 01 September 2017. https://www.merriam-webster.com/dictionary/system

Microsoft, 2006. Microsoft Security Bulletin MS06-012, Microsoft Security TechCenter. Website accessed on 17 April 2017, https://technet.microsoft.com/en-us/library/security/ms06-012.aspx

Mihramber, G.A., 1972. The modelling process. IEEE Transactions on Systems, Man, and Cybernetics, (5), pp.621-629.

Min, S., Roath, A.S., Daugherty, P.J., Genchev, S.E., Chen, H., Arndt, A.D. and Glenn Richey, R., 2005. Supply chain collaboration: what's happening?. The international journal of logistics management, 16(2), pp.237-256.

Papert, S., 1980. Mindstorms: Children, computers, and powerful ideas. Basic Books, Inc..

Moore, T. (2011) 'Why the Cabinet Office's £27bn Cyber Crime Cost Estimate is Meaningless'. Available from: https://www.lightbluetouchpaper.org/2011/02/17/why-the-cabinet-offices-27bn-cyber-crime-cost-estimate-is-meaningless/ [Accessed September 2017].

Morecroft, J.D., 1992. Executive knowledge, models and learning. European Journal of Operational Research, 59(1), pp.9-27.

Morecroft, J.D. and van der Heijden, K.A., 1992. Modelling the oil producers—Capturing oil industry knowledge in a behavioural simulation model. European journal of operational research, 59(1), pp.102-122.

Morecroft, J.D., 1982. A critical review of diagramming tools for conceptualizing feedback system models. Dynamica, 8(1), pp.20-29.

Morecroft, J.D., 2015. Strategic Modelling and Business Dynamics: A Feedback Systems Approach. John Wiley & Sons.

Mossburg, E., Fancjer, J.D., Gelinne, J., 2016. The hidden costs of an IP breach, cyber theft and the loss of intellectual property. Deloitte Review, Issue 19, pp.107-121.

Mulrow, C.D., 1987. The medical review article: state of the science. Annals of internal medicine, 106(3), pp.485-488.

Ntabe, E.N., LeBel, L., Munson, A.D. and Santa-Eulalia, L.A., 2015. A systematic literature review of the supply chain operations reference (SCOR) model application with special attention to environmental issues. International Journal of Production Economics, 169, pp.310-332.

Ocean Tomo, 2015. Annual study of intangible asset market value. March 5, 2015, website accessed on 25 April 2017: www.oceantomo.com/2015/03/04/2015-intangible-asset-market-value-study/.

Olaya, C., 2009. System dynamics philosophical background and underpinnings. In Complex Systems in Finance and Econometrics (pp. 812-832). Springer New York.

Onyeji, I., Bazilian, M. and Bronk, C., 2014. Cyber security and critical energy infrastructure. The Electricity Journal, 27(2), pp.52-60.

Orlitzky, M., Schmidt, F.L. and Rynes, S.L., 2003. Corporate social and financial performance: A meta-analysis. Organization studies, 24(3), pp.403-441.

Papachristos, G., 2012. Case study and system dynamics research: Complementarities, pluralism and evolutionary theory development. In 30th International Conference of the System Dynamics Society. http://www. systemdynamics.org/conferences/2012/proceed/papers P (Vol. 1125).

Paulsson, U., Nilsson, C.H. and Wandel, S., 2011. Estimation of disruption risk exposure in supply chains. International

Journal of Business Continuity and Risk Management, 2(1), pp.1-19.

Pearson, K., 1892. The grammar of science (Vol. 17). Walter Scott.

Perrow, C., 1984. Normal accidents: Living with high risk systems, Basic Books Inc., New York.

Peters, D.H., 2014. The application of systems thinking in health: why use systems thinking? Health Research Policy and Systems, 12(1), p.51.

Pettit, T.J., Fiksel, J. and Croxton, K.L., 2010. Ensuring supply chain resilience: development of a conceptual framework. Journal of business logistics, 31(1), pp.1-21. Plate, R. and Monroe, M., 2014. A structure for assessing systems thinking. The 2014 Creative Learning Exchange, 26, pp.1-12.

Richards, K., LaSalle, R., Devost, M., van der Dool, F., Kennedy-White, J. 2017. Cost of cybercrime study, insight on the security investments that make a difference. Ponemon Institute LLC, MI, USA.

Popper, K., 1972. “Conjectures and refutations”. Routledge and Kegan Paul Press.

Poulsen, K. 2009. Report: Cyber-attacks caused power outages in Brazil. Wired Magazine Online edition. http://www.wired.com/2009/11/brazil/.

Prentice, C.R., 2016. Why so many measures of non-profit financial performance? Analysing and improving the use of financial measures in non-profit research. Non-profit and Voluntary Sector Quarterly, 45(4), pp.715-740.

Radianti, J. and Gonzalez, J.J., 2007. A preliminary model of the vulnerability black market. In 25th International System Dynamics Conference at Boston, USA.

Rahmandad, H., Oliva, R., Osgood, N.D. and Richardson, G., 2015. Analytical Methods for Dynamic Modellers. MIT Press.

Ramo, S. and Clair, R.K.S., 1998. The systems approach: Fresh solutions to complex civil problems through combining science and practical common sense. KNI.

RAND Corporation, 2017, “Cyber warfare”, website accessed on 20 April 2017,

Randers, J. ed., 1980. Elements of the system dynamics method (edited by Jorgen Randers). Cambridge, MA: MIT press.

Reuters, 2017. Global shipping giant Maersk is reeling from the ransomware fallout. Fortune online website. Accessed 10 July 2017. http://fortune.com/2017/06/29/petya-goldeneye-maersk-ransomware-effects/

Reuters. 2012. Special Report - Cyber-crime - How can firms tackle this fast emerging invisible menace? http://www.biodiversitylibrary.org/bibliography/57908.

Reuters. 2014a. Security breach hits more prominent U.S. retailers, report says. http://www.huffingtonpost.com/2014/01/11/security-breach-more-retailers_n_4583200.html.

Reuters. 2014b. Experts warn that the global shipping industry is vulnerable to cyber-attack. South China Morning Post. http://www.scmp.com/news/world/article/1496193/experts-warn-global-shipping-industry-vulnerable-cyber-attack.

Richards, J. 2014. Denial-of-service: the Estonian cyberwar and its implications for U.S. National security. International affairs review. http://www.iar-gwu.org/node/65.

Richardson, G.P. and Pugh III, A.I., 1981. Introduction to system dynamics modelling with DYNAMO. Productivity Press Inc.

Richardson, G.P., 1991. Feedback thought in social science and systems theory. Pegasus Communications, Inc.

Richmond, B., 1976. Conceptual Monograph No.2: The outward vs. inward paradigm and the management of social systems. System Dynamics Working paper D-2456-1, 1976, System Dynamics group at the Massachusetts Institute of Technology, Cambridge, Massachusetts, USA.

Richmond, B., 1994, July. System dynamics/systems thinking: Let's just get on with it. In International systems dynamics conference, Sterling, Scotland.

Rid, T. and Buchanan, B., 2015. Attributing cyber-attacks. Journal of Strategic Studies, 38(1-2), pp.4-37.

Rocks, D., Park, A., Pascual, A.M., Little, D., Brown, J. 2001. The Net as a Lifeline. Business Week, October 29, 2001.

Rodin, J., 2014. The resilience dividend: being strong in a world where things go wrong. PublicAffairs.

Romanosky, S. (2016). Examining the Costs and Causes of Cyber Incidents. Journal of Cybersecurity, 1–15.

Rouse, W.B., 2014. Human interaction with policy flight simulators. Applied ergonomics, 45(1), pp.72-77.

Rozados, I.V. and Tjahjono, B., 2014. Big data analytics in supply chain management: Trends and related research. In 6th International Conference on Operations and Supply Chain Management.

Saunders, M., Lewis, P., Thornhill, A., 2016. "Research methods for business students", 7th edition, Pearson Learning.

Schlosser, R.W., Wendt, O. and Sigafoos, J., 2007. Not all systematic reviews are created equal: Considerations for appraisal. Evidence-Based Communication Assessment and Intervention, 1(3), pp.138-150.

Schon, D.A. and DeSanctis, V., 1986. The reflective practitioner: How professionals think in action.

Schryen, G., Wagner, G. and Benlian, A., 2015. Theory of knowledge for literature reviews: an epistemological model, taxonomy and empirical analysis of IS literature. Thirty Sixth International Conference on Information Systems, Fort Worth 2015.

Security, I., & Mcafee. 2014. Net Losses : Estimating the Global Cost of Cybercrime.

Senge, P., 1990. The fifth discipline. The Art & Practice of Learning Organization. Doupleday Currence, New York.

Senge, P.M. and Forrester, J.W., 1980. Tests for building confidence in system dynamics models. System dynamics, TIMS studies in management sciences, 14, pp.209-228.

Sheffi, Y., 2015. The power of resilience. MIT University press.

Sheffi, Y. and Rice Jr, J.B., 2005. A supply chain view of the resilient enterprise. MIT Sloan management review, 47(1), p.41.

Sheffi, Y., & Rice, J. B. (2005). A Supply Chain View of the Resilient Enterprise. MIT Sloan Management Review, 47(1), 41–48.

Sheffi, Y., & Rice, J. B. 2005. A Supply Chain View of the Resilient Enterprise. MIT Sloan Management Review, 47(1): 41–48.

Shutao, D., Xin, X.S. and Xiaoguo, Z.K., 2009. Information Technology in Supply Chains: The Value of IT-Enabled Resources Under Competition (Research Note). Information Systems Research, 20(1), pp.18-32.

Siegel, M., Moussouris, K., 2015. The Wolves of Vuln Street: the 1st Dynamic Systems model of the 0 day market. https://www.rsaconference.com/writable/presentations/file_upload/ht-t08-the-wolves-of-vuln-street-the-1st-dynamic-systems-model-of-the-0day-market_final.pdf

Smith, D.J., 2017. Reliability, maintainability and risk: practical methods for engineers. Butterworth-Heinemann.

Sterman, J.D., 1989. Modelling managerial behaviour: Misperceptions of feedback in a dynamic decision making experiment. Management science, 35(3), pp.321-339.

Sterman, J. D., 2000. “Business Dynamics”, Irwin McGraw-Hill, Boston

Sterman, J., 2014. Interactive web-based simulations for strategy and sustainability: The MIT Sloan LearningEdge management flight simulators, Part I. System Dynamics Review, 30(1-2), pp.89-121.

Sterman, J. D., Oliva, R., Linderman, K., Bendoly, E., 2015. ”System dynamics perspectives and modelling opportunities for research in Operations Management”, Journal of Operations Management.

Sterman, J., 2003. System Dynamics: systems thinking and modelling for a complex world. ESD International Symposium.

Sterman, J.D.J.D., 2000. Business dynamics: systems thinking and modelling for a complex world, McGraw-Hill / Irwin.

Sterman, J.D., 1989. Modelling managerial behaviour: Misperceptions of feedback in a dynamic decision making experiment. Management science, 35(3), pp.321-339.

Sterman, J.D. and Dogan, G., 2015. “I’m not hoarding, I’m just stocking up before the hoarders get here”: Behavioural causes of phantom ordering in supply chains. Journal of Operations Management, 39, pp.6-22.

Stevens, G.C. and Johnson, M., 2016. Integrating the Supply Chain… 25 years on. International Journal of Physical Distribution & Logistics Management, 46(1), pp.19-42.

Stoker, D. and Cooke, A., 1994, October. Evaluation of networked information sources. In Essen Symposium (pp. 287-312).

Suddaby, R., 2006. From the editors: What grounded theory is not. Academy of management journal, 49(4), pp.633-642.

Sweeney, L.B. and Sterman, J.D., 2000. Bathtub dynamics: initial results of a systems thinking inventory. System Dynamics Review, 16(4), pp.249-286.

Taormina, R., Galelli, S., Tippenhauer, N.O., Salomons, E. and Ostfeld, A., 2017. Characterizing Cyber-Physical Attacks on Water Distribution Systems. Journal of Water Resources Planning and Management, 143(5), p.04017009.

Tatum, C.B., 1987. Improving constructability during conceptual planning. Journal of Construction Engineering and Management, 113(2), pp.191-207.

Taylor, F.W., 1914. Scientific management. The Sociological Review, 7(3), pp.266-269.

Teuteberg, F. and Wittstruck, D., 2010. A systematic review of sustainable supply chain management. Multikonferenz Wirtschaftsinformatik 2010, p.203.

Thomas, W.I., Thomas, D. S., (1928): The child in America: behaviour problems and programs. New York, Alfred Knopf.

Thornton, A. and Lee, P., 2000. Publication bias in meta-analysis: its causes and consequences. Journal of clinical epidemiology, 53(2), pp.207-216.

Tierney, K. and Bruneau, M., 2007. Conceptualizing and measuring resilience: A key to disaster loss reduction. TR news, (250).

Tranfield, D., Denyer, D. and Smart, P., 2003. Towards a methodology for developing evidence-informed management knowledge by means of systematic review. British journal of management, 14(3), pp.207-222.

Turner, B.L., Menendez, H.M., Gates, R., Tedeschi, L.O. and Atzori, A.S., 2016. System dynamics modelling for agricultural and natural resource management issues: review of some past cases and forecasting future roles. Resources, 5(4), p.40.

Vazquez, M. and Liz, M., 2007, July. System dynamics and philosophy: A constructivist and expressivist approach. In Proceedings of the international conference of the system dynamics society.

Venkatraman, N. and Ramanujam, V., 1986. Measurement of business performance in strategy research: A comparison of approaches. Academy of management review, 11(4), pp.801-814.

Vennix, J.A. and Gubbels, J.W., 1992. Knowledge elicitation in conceptual model building: A case study in modelling a regional Dutch health care system. European journal of operational research, 59(1), pp.85-101.

Vennix, J.A., 1996. Group model building: facilitating team learning using system dynamics (No. 658.4036 V4).

Verscheure, K., Kyllo, A.K., Filzwieser, A., Blanpain, B. and Wollants, P., 2006, January. Furnace cooling technology in pyrometallurgical processes. In Sohn International Symposium; Advanced Processing of Metals and Materials Volume 4: New, Improved and Existing Technologies: Non-Ferrous Materials Extraction and Processing (Vol. 4, pp. 139-153).

Von Bertalanffy, L., 1968. General system theory. New York, 41973(1968), p.40.

Voss, C., Johnson, M. and Godsell, J., 2015. Revisiting case research in operations management. In 22nd International Annual EurOMA Conference.

Wagstaff, J., 2014. All at sea: global shipping fleet exposed to hacking threat. Reuters technology news website. Accessed on 17 August 2016: https://www.reuters.com/article/us-cybersecurity-shipping/all-at-sea-global-shipping-fleet-exposed-to-hacking-threat-idUSBREA3M20820140423

Waring, S.P., 2016. Taylorism transformed: Scientific management theory since 1945. UNC Press Books.

Warren, M. and Hutchinson, W., 2000. Cyber-attacks against supply chain management systems: a short note. International Journal of Physical Distribution & Logistics Management, 30(7/8), pp.710-716.

Webster, S.T., 2009. Principles of supply chain management. Dynamic Ideas.

Webster, J. and Watson, R.T., 2002. Analysing the past to prepare for the future: Writing a literature review. MIS quarterly, pp. xiii-xxiii.

WEF. 2012. Partnering for Cyber-resilience. http://www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf.

WEF. 2013. Building Resilience in Supply Chains.

WEF. 2013. Building Resilience in Supply Chains.

WEF. 2015. Partnering for Cyber-resilience - Towards the Quantification of Cyber Threats. http://www.weforum.org/reports/partnering-cyber-resilience-towards-quantification-cyber-threats.

Weinberg, G.M., 1975. An introduction to general systems thinking. New York: Wiley.

White, D., 1995. Application of systems thinking to risk management: a review of the literature. Management Decision, 33(10), pp.35-45.

Wichowski, D.E. and Kohl, L.E., 2012. Establishing credibility in the information jungle: Blogs, microblogs, and the CRAAP test. Online credibility and digital ethos: Evaluating computer-mediated communication, pp.229-251.

Wiener, N., 1948. Cybernetics. Scientific American, 179(5), pp.14-19.

Wikileaks, 2017. Vault 7: CIA Hacking tools revealed. Website accessed on 10 April 2017, https://wikileaks.org/ciav7p1/

Wilding, N., 2016. Cyber-resilience: How important is your reputation? How effective are your people? Business Information Review, 33(2), pp.94-99.

Will M. Bertrand, J. and Fransoo, J.C., 2002. Operations management research methodologies using quantitative modelling. International Journal of Operations & Production Management, 22(2), pp.241-264.

Williams, L.R., Esper, T.L. and Ozment, J., 2002. The electronic supply chain: Its impact on the current and future structure of strategic alliances, partnerships and logistics leadership. International Journal of Physical Distribution & Logistics Management, 32(8), pp.703-719.

Windelberg, M., 2016. Objectives for managing cyber supply chain risk. International Journal of Critical Infrastructure Protection, 12, pp.4-11.

Wolstenholme, E.F., 2003. Towards the definition and use of a core set of archetypal structures in system dynamics. System Dynamics Review, 19(1), pp.7-26.

Wong, J.C., Solon, O., 2017. Massive ransomware cyber-attack hits nearly 100 countries around the world. The Guardian. Accessed on 20 May 2017. https://www.theguardian.com/technology/2017/may/12/global-cyber-attack-ransomware-nsa-uk-nhs

Yin, R. K., 1994. ”Case Study Research: case and methods”. Sage publications.

Zetter, K., 2014. Countdown to zero day: Stuxnet and the launch of the world's first digital weapon. Broadway Books.

Zhu, B., Joseph, A. and Sastry, S., 2011a, October. A taxonomy of cyber-attacks on SCADA systems. In Internet of things (iThings/CPSCom), 2011 international conference on and 4th international conference on cyber, physical and social computing (pp. 380-388). IEEE.

Zhu, Q. and Başar, T., 2011, December. Robust and resilient control design for cyber-physical systems with an application to power systems. In Decision and Control and European Control Conference (CDC-ECC), 2011 50th IEEE Conference on (pp. 4066-4071). IEEE.

Zobel, C.W. and Khansa, L., 2014. Characterizing multi-event disaster resilience. Computers & Operations Research, 42, pp.83-94.

Zorn, T. and Campbell, N., 2006. Improving the writing of literature reviews through a literature integration exercise. Business Communication Quarterly, 69(2), pp.172-183.

11 Appendix

11.1 Glossary of terms

This glossary gathers the terminology that has been used in this thesis in regard to cyber-risk and resilience in the global supply chain. It was found convenient to include this glossary, as the audiences that will be reading this work come from a variety of backgrounds, including SCM, ITM, and R&RM for example. The sources have been indicated as far as possible from scientific sources, otherwise the relevant practitioner magazines or news outlet websites have been mentioned.

Accident (w.r.t. Safety)	An undesired and unplanned (but not necessarily unexpected) event that results in at least a specified level of loss (Leveson, 1995), such as loss of human life or human injury, property damage, environmental pollution, mission loss, and economic loss. (Leveson, 2011)
Adaptability	Capacity of a Supply Chain to adjust its structure to changes in its environment, by developing new plans, taking new actions or by modifying behaviours. Closely related to *Flexibility*. Considered by some authors as one of the five characteristics of resilience (Rodin, 2014).

CISO – Chief Information Security Officer	A title associated with the highest ranking individual whose sole function within an organization is to manage an organization-wide security program (Bayuk et al., 2012).
Computer emergency response team (CERT)	An organization whose mission is to receive reports of cyber incidents and gather a team qualified and motivated to resolve them (Bayuk et al., 2012).
Crimeware	Software created for executing cybercrimes as a service, e.g., denial of service attacks.
Cryptocurrency	It is a medium of exchange using cryptographic systems to both secure transactions, and to control the creation of additional units of the currency. It is considered a digital asset. Some of the more successful cryptocurrencies include Bitcoin, and more recently, Ethereum.
Cryptology	It is the science of code and cypher systems, widely used to protect communications. Techniques such as end-to-end encryption have become a standard in the protection of digital information transfer.
Cryptographic systems	Communication systems which apply cryptological techniques to their communication protocols.
Current Supply Chain	Network structure and configuration of the supply chain that considers the Agents, Infrastructure, Procedures and Protocols necessary for its steady state operation.

Cyber-physical system	[Definition Pending]
Cyber-risk	Business *Risk*s derived from the interaction of information technology and supply chain operations.
Cyber-security	It is the ability to control access to networked systems, and the information they contain, referring to methods of using people, process and technology to prevent, detect and recover from damage to confidentiality, integrity and availability of information in cyber space (Bayuk et al., 2012). Cyber-security includes the overall coordinated measures and actions taken by potential targets to prevent, prepare, analyse and respond to the threats their information systems are facing due to cyber-attacks (Katz, 2013).
Cyber-space	The global collection of electronic circuits which allow people and systems to connect without physical proximity or connectivity.
Cyber-warfare	Actions by a nation-state or international organization to attack and attempt to damage another nation's computer or information networks through, for example, computer viruses or denial-of-service attacks [RAND 2017]
Cyber-weapon	Malicious software that can be used to access host computer networks by a foreign agent, for the purpose of gathering strategic information or to cause disruption in the activities of the host

Disruption	Conditions that will cause a supply chain event, process or activity to vary beyond its thresholds of normality.
Disruption, deliberate	A *Disruption* that is intentionally generated to provoke change through the *Adaptability* of the supply chain without destabilizing the whole system, or to lose its ability to self-regulate.
Disruption Period	Time over which the influence of a disruption is experienced in a supply chain. This period begins at the start of the Disruption Trigger and continues until the moment when the supply chain has a performance value and trend within its normal functioning variability.
Disruption Trigger	Event when an External Disruptor acts upon an exposed Supply chain interphase.
Disruptive Event	Event when a *Disruption* is occurring in a supply chain.
Error (w.r.t. Safety)	A design flaw or a deviation from a desired or intended state (Leveson, 1995)
External Disruptor	Agent external to the *Current supply chain* which as the ability of acting upon a *Supply chain interphase* to cause a *Disruption*.
Flexibility	Capacity of a supply chain to apply existing resources to new or additional purposes or roles. Closely related to *Adaptability*.
Operative Module	Set of self-contained operations within a supply chain that can be combined, through their *Supply chain*

	interphases, to form more complex supply chain structures.
Phishing	Use of electronic communication such as emails or webpages to fraudulently attempt to obtain confidential information from an unsuspecting party. Information sought may include user names, passwords and credit card details, for example.
Reliability (Safety)	The probability that a component of a system will perform its intended purpose for a specific time and under specific environmental conditions (Leveson, 1995)
Resilience	It is the ability of a supply chain to continue its activities during and after a disrupting event, with as little disruption to its downstream performance as possible. It is a dynamic concept that is measured and evaluated over the Disruption Period. Other definitions include: "The ability of a system to return to its original state or move to a new, more desirable state after being disturbed" (Christopher et al., 2003), "Shock absorption between stages in the supply chain" (Sheffi & Rice, 2005). Concept originally borrowed from Materials engineering as a measure of the quantity of energy that can be absorbed by a material without creating a permanent distortion (Marks, 2016).
Risk	Exposure or lack of protection to danger harm or loss from a Disruptive Event. This exposure is created by the structure of the supply chain. Risk is a static concept,

	and its description and quantification say nothing about how it will dynamically react to a *Disruption*.
Socio Technical Systems (STS)	It is an approach to complex organizational work design that recognizes the interaction between people and technology in workspaces. The notion of STS was created in the context of labour studies by the Tavistock institute in London at the end of the 1950's (Emery et al., 1960).
Spoofing	An event whereby a hacker successfully passes as a different member of the supply process by falsifying some data, and thereby gaining an illegitimate advantage
Supply chain interphase	Transition point in a supply chain where there is exchange of goods or information between two established *Operative Modules*, and with option of human influence.
System Dynamics	For a supply chain, it is the characteristic that supply chain structure leads to its endogenous behaviour over time, and that this system structure in constituted by processes with non-linear causal relationships, feedback loops, delays and inertia generators.
Zero-Day Vulnerability	An undisclosed or unknown vulnerability in computer software that becomes known only when hackers have made use of it to cause adverse effects. It is called zero-day because, due to lack of information, the software author has no time (zero-day) to develop a patch or

	workarounds to mitigate its effects before the attack is carried out. An example of a famous case that features the use of zero-day vulnerabilities is the Stuxnet attack (Kushner, 2013) which used 6 different zero-day vulnerabilities to disable control systems in the Programmable Logic Controllers (PLC) different nuclear plants.

11.2 Research protocol – Dynamic model

v.161121

DTU

PhD project – Managing Cyber risk in the global supply chain

Research Protocol for study "Dynamic simulation of response to cyber risks"

I. Objectives

The objective of this research protocol is to describe and prescribe a reproducible data gathering and analysis process in the context of the PhD research project "Managing cyber risk in the global supply chain". This research has the sponsorship of the Department of Management Engineering at the Technical University of Denmark DTU and is performed in collaboration with the System Dynamics group at the Massachusetts Institute of Technology. This process results in the development of a series of representations of the dynamic (time-dependent) structure and response of a supply chain when faced with a cyber-attack. These representations are causal loop diagrams, a hierarchical control structure and a system dynamics model.

The purpose of the study is threefold: 1) to gain some insight into the supply chain structures that partake during a cyber-attack, 2) to understand the relationship of this structure the organizational reaction and performance to the cyber-attack, and 3) to identify and test the main factors that influence that reaction and performance.

As a source of information, this study will use semi-structured interviews and the gathering of documentation. This information will have both relation to the structure of the supply chain and the cyber-attack incident that required a response. The required characteristics of the structure include information flows, information storage, regulating loops, delays, and the potential perturbations to the system. Information about the incident includes a description of the events and performance indicators during the event.

The subjects of this research are organizational members with knowledge about the supply chain processes and who have experienced the cyber-risk incident.

The research question guiding this research protocol is:

"How can system dynamics simulation mitigate compartmentalization, static frameworks and historical dependence for managing cyber risks in the supply chain?"

II. Background and Rationale

Supply Chain processes are the physical movement of goods and services interdependent between human operators and information technology, processes that are based on an underlying structure of coordinating information flows in the organization (Forrester, 1961; Sahin et al., 2002).

Disruptors to these coordinating information flows, such as cyber-attacks, can result in operational disruptions for cases where the supply chain reaction is insufficient. There is limited understanding about the relationship between underlying information structures in the supply chain, the risk these pose to supply

Research Protocol page 1 of 4 PhD Project

chain operations for the case of an information flow disruption, and the reaction these supply chains adopt when faced with these disruptions.

This study seeks to contribute to the scientific development of a framework for understanding resilient behavior. The approach of using system dynamics starts from the premise that organizational structure is the source of its visible behavior, and that by understanding the structure it is possible to experiment with different operating conditions, and as a result provides information to design the required system behavior.

Therefore, the application of this method delivers results that show its capacity to address compartmentalization, static versus dynamic behavior description, and historical dependence during its application. The analysis of this capacity, for example its range or limitations, provides information to answer the underlying research question guiding this research protocol.

III. Process

A. Research Design

The research is a descriptive, correlational and meta-analytical case study of a supply chain case.

- It is descriptive as the data that will be gathered will mostly be a categorical non-numerical detail of the components of the supply chain;
- it is correlational as the analysis will look for the relationship between different components of the described structure and the types of responses these supply chains have during disruptions, and data will be gathered from multiple roles in the supply chain to decrease the threat if internal validity, i.e., minimizing the systematic error (bias) in the data that is gathered;
- it is meta analytical as the study considers the gathering of data from, and the comparative analysis of, multiple companies so as to decrease the threat of external validity, i.e., the capacity of generalizing the results of this research to organizations that did not take part in the research.

This research expected to reveal mechanisms and reveal causalities, and generalizability is not an aim of the study at this stage, rather the in-depth study of a specific case.

B. Interview structure

The interview is a semi-structured interview to obtain the information required for the analysis. The guiding questions are:

1. Please describe the normal operation of the area
2. Please describe the cyber-attack event
3. Which persons and areas participated in containing the attack?
4. How was the attack contained (agents, actions, time, resources)?
5. Which persons and areas participated in the recovery after the attack?
6. How was the recovery carried out (agents, actions, time, resources)?
7. Why do you think the attack happened?
8. How could the organization have prevented the attack?
9. How well do you think the company reacted to the attack?

v.161121

It is a semi-structured interview because any of these questions may lead to a deeper discussion into the dynamics of the organization under normal conditions or under cyber-attack.

During the interviews, causal loops can be drawn to describe the causalities present in the narrative that is being collected.

C. Data Analysis

The Additional to the problem statement, the following tools and analyses are used, according to extant literature (Sterman, 2000; Morecroft, 2015) are three representational tools

- The problem statement and case description identifies the problem description, time horizon applicable to the problem, and the dynamic problem description (also known as modes of reference),
- The causal loop diagram identifies system variables, causal relationships between variables, polarities in these causal relationships, feedback loops, feedback loop types, relevant delays in the causal relationships, and allows the identification of endogenous and exogenous variables to the system. These elements from the causal loop diagram give rise to a narration of an hypothesis for the occurrence of the reference mode.
- The hierarchical control structure identifies the organizational sectors involved in the problem, the control loops designed into the system, the control actions and controllers, and the hierarchical levels of the system.
- The system dynamics model incorporates the information from the causal loops and hierarchical control structure into a quantifiable model, by additionally identifying the stock and flows relevant to the problem, quantifying the causal relationships, and generating a dynamic (time-dependent) behavior of the system through simulation.

D. Sample

The data will be gathered from as many of the following roles as possible in the supply chain:

- Supply chain manager
- IT manager
- Principal buyer
- Outbound specialist
- Warehouse manager / operator
- Finance
- External consultants

E. Measurement / Instrumentation

This study will use one instruments for the recording and measurement of the data.

- C1.- Semi structured interview

F. Study process

- Request an schedule interview
- Perform interview
- Record data

- Analyze data
- Report the results

G. Threats to Validity

The threat to internal validity is addressed by the data gathering from different roles in the supply chain in independent interviews, so as to decrease systematic errors ,i.e., bias.

The threat to external validity not addressed by this study, as it is an exploratory and revelatory study, thus the generalizability is not an objective of the research at this stage.

IV. Bibliography

Forrester, J., 1961. Industrial Dynamics, System Dynamics Series, Pegasus Communications.

Leveson, N., 2011. Engineering a safer world: Systems thinking applied to safety. MIT press.

Rowley, J., 2012. Conducting research interviews. Management Research Review, 35(3/4), pp.260-271.

Sahin, F. and Robinson, E.P., 2002. Flow coordination and information sharing in supply chains: review, implications, and directions for future research. Decision sciences, 33(4), pp.505-536.

11.3 List of Unsafe Control Actions (UCA)

CA Description	Source	Destination	UCA
Confirm payment order	Plant's Bank	Plant	Not providing Order Payment Confirmation when there has been a supplier payment order is hazardous
Confirm payment order	Plant's Bank	Plant	Providing Order Payment Confirmation when there has not been a supplier payment order is hazardous
Confirm payment order	Plant's Bank	Plant	Providing Order Payment Confirmation before there has been a supplier payment order is hazardous
Order Supplier payment	Plant	Plant's Bank	Not providing Supplier Payment Order when there has been confirmation of product reception and validation is hazardous
Order Supplier payment	Plant	Plant's Bank	Providing Supplier Payment Order when there has not been a product reception is hazardous
Order Supplier payment	Plant	Plant's Bank	Providing Supplier Payment Order when there has not been product validation is hazardous
Order Supplier payment	Plant	Plant's Bank	Providing Supplier Payment Order before there has been product reception is hazardous
Order Supplier payment	Plant	Plant's Bank	Providing Supplier Payment Order before there has been product validation is hazardous
Order Supplier payment	Plant	Plant's Bank	Providing Supplier Payment Order when there has not been a supplier payment data confirmation is hazardous

CA Description	Source	Destination	UCA
Cancel supplier payment	Plant	Plant's Bank	Not providing Supplier Payment Cancellation when there has not been product reception is hazardous
Cancel supplier payment	Plant	Plant's Bank	Providing Supplier Payment Cancellation when there has been product validation, reception and supplier data confirmation is hazardous
Cancel supplier payment	Plant	Plant's Bank	Not providing Supplier Payment Cancellation when there has not been product validation is hazardous
Cancel supplier payment	Plant	Plant's Bank	Not providing Supplier Payment Cancellation when there has not been a supplier payment data confirmation is hazardous
Activate Purchase Order	Plant	Supplier	Not providing Purchase Order Activation when there has been a confirmed requirement is hazardous
Activate Purchase Order	Plant	Supplier	Providing Purchase Order Activation when there has not been a confirmed requirement is hazardous
Activate Purchase Order	Plant	Supplier	Providing Purchase Order Activation before there has been a confirmed requirement is hazardous
Activate Purchase Order	Plant	Supplier	Providing Purchase Order Activation when the supplier has not been confirmed is hazardous
Activate Purchase Order	Plant	Supplier	Providing Purchase Order Activation before the supplier

CA Description	Source	Destination	UCA
			has been confirmed is hazardous
Cancel Purchase Order	Plant	Supplier	Providing Purchase Order Cancellation when the purchase order is correct is hazardous
Cancel Purchase Order	Plant	Supplier	Not providing Purchase Order Cancellation when the supply process is incorrect is hazardous
Cancel Purchase Order	Plant	Supplier	Providing Purchase Order Cancellation after pickup has been executed is hazardous
Validate Product	Plant	Supplier	Not providing Product Validation when there has been a product and documentation reception is hazardous
Validate Product	Plant	Supplier	Providing Product Validation when there has not been a product and documentation reception is hazardous
Validate Product	Plant	Supplier	Providing Product Validation with the wrong documentation is hazardous
Validate Product	Plant	Supplier	Providing Product Validation before there has been a product and documentation reception is hazardous
Validate Product	Plant	Supplier	Providing Product Validation without quality approval is hazardous
Perform Delivery	Transport	Plant	Not providing product delivery when a schedule has been agreed is hazardous
Perform Delivery	Transport	Plant	Providing product delivery when a schedule has not been agreed is hazardous

CA Description	Source	Destination	UCA
Perform Delivery	Transport	Plant	Providing product delivery with the wrong documentation is hazardous
Perform Delivery	Transport	Plant	Providing product delivery when the address has not been confirmed is hazardous
Perform Delivery	Transport	Plant	Providing product delivery when the address data has been changed is hazardous
Perform Delivery	Transport	Plant	Providing product delivery to the incorrect address is hazardous
Perform Delivery	Transport	Plant	Providing product delivery before a schedule has been agreed is hazardous
Perform Delivery	Transport	Plant	Providing product delivery before correct documentation has been issued is hazardous
Perform Delivery	Transport	Plant	Providing product delivery before the correct address has been confirmed is hazardous
Perform Delivery	Transport	Plant	Providing product delivery when the product is incorrect is hazardous
Receive product	Plant	Transport	Not providing product reception when correct documentation and quality has been confirmed is hazardous
Receive product	Plant	Transport	Providing product reception when the incorrect documentation has been received is hazardous
Receive product	Plant	Transport	Providing product reception when quality testing has not been granted is hazardous

CA Description	Source	Destination	UCA
Receive product	Plant	Transport	Providing product reception for the incorrect product is hazardous
Receive product	Plant	Transport	Providing product reception when the supplier has not been confirmed is hazardous
Receive product	Plant	Transport	Providing product reception after the order has been cancelled is hazardous
Receive product	Plant	Transport	Providing product reception before the correct documentation has been received is hazardous
Receive product	Plant	Transport	Providing product reception before the quality testing has been granted is hazardous
Receive product	Plant	Transport	Providing product reception before the correct product has been identified is hazardous
Receive product	Plant	Transport	Providing product reception before the correct supplier has been confirmed is hazardous
Perform inbound check	Plant	Transport	Not performing inbound check when the product and documentation has been received is hazardous
Perform inbound check	Plant	Transport	Performing inbound check when the incorrect product has been identified is hazardous
Perform inbound check	Plant	Transport	Performing inbound check when the incorrect documentation has been received is hazardous
Perform inbound check	Plant	Transport	Performing inbound check with an incomplete process is hazardous

CA Description	Source	Destination	UCA
Perform inbound check	Plant	Transport	Performing inbound check without the correct experience is hazardous
Perform inbound check	Plant	Transport	Preforming inbound check before the correct product has been identified is hazardous
Perform inbound check	Plant	Transport	Performing inbound check before the correct documentation has been received is hazardous
Perform inbound check	Plant	Transport	Performing inbound check before the correct process has been completed is hazardous
Perform inbound check	Plant	Transport	Performing inbound check before the correct experience has been obtained is hazardous
Confirm Purchase Order	Supplier	Plant	Not providing purchase order confirmation when the buyer, product and timeframes have been confirmed is hazardous
Confirm Purchase Order	Supplier	Plant	Providing purchase order confirmation when the buyer has not been confirmed is hazardous
Confirm Purchase Order	Supplier	Plant	Providing purchase order confirmation when the product has not been confirm is hazardous
Confirm Purchase Order	Supplier	Plant	Providing purchase order confirmation when the timeframe has not been confirmed is hazardous
Confirm Purchase Order	Supplier	Plant	Providing purchase order confirmation before the buyer has been confirmed is hazardous

CA Description	Source	Destination	UCA
Confirm Purchase Order	Supplier	Plant	Providing purchase order confirmation before the product has been confirmed is hazardous
Confirm Purchase Order	Supplier	Plant	Providing purchase order confirmation before the timeframe has been confirmed is hazardous
Confirm Purchase Order	Supplier	Plant	Providing purchase order confirmation when the purchase order has been cancelled is hazardous
Confirm Purchase Order Cancellation	Supplier	Plant	Not providing purchase order cancellation when the instruction ahs been sent by buyer is hazardous
Confirm Purchase Order Cancellation	Supplier	Plant	Providing purchase order cancellation when the instruction has not been issued by the buyer is hazardous
Send Documentation	Supplier	Plant	Not providing product documentation when the product pickup takes place is hazardous
Send Documentation	Supplier	Plant	Providing product documentation to the wrong buyer can be hazardous
Send Documentation	Supplier	Plant	Providing product documentation before the correct buyer data has been confirmed is hazardous
Send Documentation	Supplier	Plant	Providing transport documentation before the correct transport agent data has been confirmed is hazardous

CA Description	Source	Destination	UCA
Send Documentation	Supplier	Plant	Providing incomplete product documentation is hazardous
Confirm Transport Payment Order	Supplier's Bank	Supplier	Not providing transport payment order when there a product delivery confirmation is hazardous
Confirm Transport Payment Order	Supplier's Bank	Supplier	Providing the transport payment order to the wrong Transport Agent is hazardous
Confirm Transport Payment Order	Supplier's Bank	Supplier	Providing transport payment order for the incorrect amount is hazardous
Confirm Transport Payment Order	Supplier's Bank	Supplier	Providing transport payment order without the documentation is hazardous
Confirm Transport Payment Order	Supplier's Bank	Supplier	Providing the transport payment order before the transport Agent Data has been confirmed is hazardous
Confirm Transport Payment Order	Supplier's Bank	Supplier	Providing the transport order payment without having confirmed Transport agent Data is hazardous
Confirm Transport Payment Order	Supplier's Bank	Supplier	Providing the transport payment order before the correct documentation has been confirmed is hazardous
Confirm Transport Payment Order Cancellation	Supplier's Bank	Supplier	Not providing transport payment order cancellation when there has been an incorrect/incomplete product delivery, is hazardous
Confirm Transport Payment Order Cancellation	Supplier's Bank	Supplier	Providing transport payment order cancellation when there has been correct/complete product delivery, is hazardous

CA Description	Source	Destination	UCA
Confirm Transport Payment Order Cancellation	Supplier's Bank	Supplier	Providing transport payment order cancellation when there has been a false report of incomplete product delivery is hazardous
Confirm Transport Payment Order Cancellation	Supplier's Bank	Supplier	Providing transport payment order cancellation before the correct product delivery has been confirmed, is hazardous
Confirm Transport Payment Order Cancellation	Supplier's Bank	Supplier	Providing transport payment order cancellation before the incomplete product delivery has been confirmed is hazardous
Order Transport Payment	Supplier	Supplier's Bank	Not providing transport payment order
Transfer funds to Transport	Supplier's Bank	Transport	Not providing transfer of funds to transport when delivery has been confirmed is hazardous
Transfer funds to Transport	Supplier's Bank	Transport	Providing transfer of funds to transport when delivery has not been confirmed is hazardous
Transfer funds to Transport	Supplier's Bank	Transport	Providing transfer of funds to transport before delivery has been confirmed is hazardous
Transfer funds to Transport	Supplier's Bank	Transport	Providing transfer of funds to transport after a faulty reception has been confirmed is hazardous
Transfer funds to Transport	Supplier's Bank	Transport	Providing transfer of funds to transport before the correct transport agent data has been confirmed, is hazardous
Transfer funds to Transport	Supplier's Bank	Transport	Providing transfer of funds to transport to the incorrect transport agent is hazardous

CA Description	Source	Destination	UCA
Transfer funds to Transport	Supplier's Bank	Transport	Providing transfer if funds for the incorrect amount is hazardous
Transfer funds to Transport	Supplier's Bank	Transport	Providing transfer of funds before the correct payment amount has been confirmed is hazardous
Transfer funds to supplier	Plant's Bank	Supplier's Bank	Not providing transfer of funds to supplier when there has been confirmation of delivery is hazardous
Transfer funds to supplier	Plant's Bank	Supplier's Bank	Providing transfer of funds to supplier when delivery has not been confirmed is hazardous
Transfer funds to supplier	Plant's Bank	Supplier's Bank	Providing transfer of funds to supplier to the incorrect supplier is hazardous
Transfer funds to supplier	Plant's Bank	Supplier's Bank	Providing transfer of funds to supplier for the incorrect amount is hazardous
Transfer funds to supplier	Plant's Bank	Supplier's Bank	Providing transfer of funds to supplier before delivery has been confirmed is hazardous
Transfer funds to supplier	Plant's Bank	Supplier's Bank	Providing transfer of funds to supplier after a faulty reception is hazardous
Transfer funds to supplier	Plant's Bank	Supplier's Bank	Providing transfer of funds to supplier before the correct supplier has been confirmed is hazardous
Transfer funds to supplier	Plant's Bank	Supplier's Bank	Providing transfer of funds to supplier before the correct payment amount has been confirmed is hazardous

CA Description	Source	Destination	UCA
Activate Service Order	Supplier	Transport	Not providing a service order activation when there has been a purchase order confirmation is hazardous
Activate Service Order	Supplier	Transport	Providing a service order activation when there has not been a purchase order confirmation, is hazardous
Activate Service Order	Supplier	Transport	Providing a service order activation before there has been a purchase order confirmation is hazardous
Activate Service Order	Supplier	Transport	Providing a service order activation when there has not been a purchase order cancellation is hazardous
Activate Service Order	Supplier	Transport	Providing a service order activation when there has not been a transport agent confirmation is hazardous
Activate Service Order	Supplier	Transport	Providing a service order activation after there has been a purchase order cancellation is hazardous
Activate Service Order	Supplier	Transport	Providing a service order activation to the wrong transport agent is hazardous
Activate Service Order	Supplier	Transport	Providing a service order activation before there has been a transport agent confirmation is hazardous
Activate Service Order	Supplier	Transport	Providing a service order confirmation before the correct transport agent has been identified is hazardous

CA Description	Source	Destination	UCA
Cancel Service Order	Supplier	Transport	Not providing service order cancellation when there has been a purchase order cancellation is hazardous
Cancel Service Order	Supplier	Transport	Providing service order cancellation when there has been a false Purchase Order Cancellation is hazardous
Cancel Service Order	Supplier	Transport	Providing service order cancellation before there has been a confirmation of purchase order cancellation is hazardous
Cancel Service Order	Supplier	Transport	Providing service order cancellation after there has been product pickup is hazardous
Cancel Service Order	Supplier	Transport	Providing service order cancellation to the wrong service order is hazardous
Cancel Service Order	Supplier	Transport	Providing service order cancellation by multiple persons is hazardous
Handover transport documentation to transport	Supplier	Transport	Not providing transport documentation when the product pickup takes place is hazardous
Handover transport documentation to transport	Supplier	Transport	Providing incomplete transport documentation is hazardous
Handover transport documentation to transport	Supplier	Transport	Providing transport documentation to the wrong transport agency is hazardous

CA Description	Source	Destination	UCA
Handover transport documentation to transport	Supplier	Transport	Providing transport documentation before the correct transport agent has been confirmed is hazardous
Handover transport documentation to transport	Supplier	Transport	Providing transport documentation before it has been checked for completeness is hazardous

11.4 Time series for sales and Profit Gap

Mes	Sales Gap	Profit Gap
0	0	0
1	0	0
2	-0,05	-0,1
3	-0,3	-0,25
4	-0,7	-0,36
5	-0,75	-0,5
6	-0,8	-0,55
7	-0,65	-0,6
8	-0,4	-0,8
9	-0,15	-0,95
10	-0,17	-1,22
11	0,05	-1,5
12	0	-1,35
13	0,02	-1,4
14	0	-1,3
15	-0,02	-1,2
16	0	-1,15
17	-0,04	-1,03
18	0	-1
19	0	-0,8
20	0	-0,85
21	0,02	-0,8
22	0,04	-0,7
23	0	-0,6
24	0,02	-0,55
25	0	-0,48
26	0	-0,49
27	-0,03	-0,46
28	0	-0,44
29	-0,03	-0,42
30	0	-0,48
31	0	-0,3

Mes	Sales Gap	Profit Gap
32	0,01	-0,4
33	0	-0,4
34	-0,03	-0,41
35	-0,04	-0,38
36	0	-0,3
37	0	-0,31
38	0	-0,25
39	0,02	-0,26
40	0,04	-0,27
41	0,04	-0,27
42	-0,01	-0,26
43	0	-0,26
44	-0,04	-0,3
45	0	-0,25
46	0	-0,24
47	-0,01	-0,24
48	0	-0,23
49	0,03	-0,2
50	0	-0,08
51	0	-0,1
52	0	-0,06
53	-0,05	-0,05
54	-0,04	-0,02
55	0	0
56	0	-0,06
57	0,01	0,03
58	0	-0,02
59	0,03	0
60	0	0

11.5 Dynamic model equations

Actual Costs=
Marketing Promotion*Marketing Rate+10*Resources
Units: USD/Month
Costs in the company, simplified as consisting of resource costs plus IP management costs

Actual Profit=
Actual Sales-Actual Costs
Units: USD/Month
Actual profit level, calculated as the difference between Actual Sales and Actual Costs.

Actual Sales=
Demand*Effect of Demand
Units: USD/Month
Actual sales resulting from a demand.

Alpha=
0.4
Units: Dmnl [0,3,0.01]
Cobb-Douglas Exponent

Cobb Constant=
8.5
Units: USD/(Month*IPUnits)
Cobb-Douglas Constant

Customer Adjustment Time=
6
Units: Month
Time over which the demand is adjusted as a result of Marketing efforts

Customer Change Rate=
(Target Demand-Demand)/Customer Adjustment Time
Units: USD/(Month*Month)
Rate of change in the demand

Demand=
INTEG (Customer Change Rate, 22106.1)
Units: USD/Month
Demand level as a rate of purchase per month

Effect of Demand=
0.2
Units: Dmnl [0,5,0.1]
The effect of demand on sales is consdiered as proportional.

Exclusive IP=
INTEG ("R&D Projects"-IP Rights Expiration, 0.4*Planned IP*IP Lifetime/(IP Lifetime+IP Creation Time))
Units: IPUnits
Exclusive IP in the company

Expected Sales=
4421.21
Units: USD/Month
Expected Sales according to company planning

IP Creation Time=
6
Units: Month
Average time that it takes the researcher to develop an IPUnit

IP Gap=
MAX(0,Planned IP-Exclusive IP)
Units: IPUnits
Difference between the planned Exclusive IP level and the Actual exclusive IP level

IP Lifetime=
240
Units: Month
Average number of months that ABC industries has property over its IP. Considered as 20 years.

IP Rights Expiration=
Exclusive IP/IP Lifetime
Units: IPUnits/Month
Rate of expiration of IP Units.

Marketing Factor=
2000
Units: USD/(Month*Hours) [0,10000,100]
Effect on the resulting demand.as USD/Month of each hour of Marketing effort

Marketing Promotion=
INTEG (Marketing Promotion change rate, 0)

Units: Hours
Number of marketing hours

Marketing Promotion adjustment time=
12
Units: Month
Time required by the marketing departmetn to adjust the marketing efforts. Normally based in an annual plan

Marketing Promotion change rate=
(10*Required Marketing-Marketing Promotion)/Marketing Promotion adjustment time
Units: Hours/Month
Change rate at which the marketing hours are adjusted

Marketing Rate=
0.5
Units: USD/(Hours*Month)
Rate at which Marketing service are hired.

Planned IP=
1000
Units: IPUnits
Number of IP units that are expected to account for a big enough differentiation that results in the expected sales level

"R&D Effectiveness"=

0.02
Units: IPUnits/(USD*Researcher)
The number of IP units that can be produced by each researcher and by each dollar invested.

"R&D Projects"=
MIN(Resources*"R&D Effectiveness"*Actual Profit,IP Gap/IP Creation Time)
Units: IPUnits/Month
Rate of Production of IP. This is determined as the minimum between the available producion due to the available profit and the required IP production.

Required Marketing=
WITH LOOKUP (Sales Gap,([(-1.4,0)-(1,21)],(-1.4,20),(-1.30581,20), (-1.09602,19.25), (-0.916208,16.6711),(-0.809174,13.0789),(-0.749235,8.8421),(-0.646483,4.69737),(0.535168,2.30263),(-0.346789,0.552632),(-0.119878,0.0921053),(0,0),(1,0)))

Units: Hours
Required marketing as resulting from the underlying Sales Gap

Resources=
50
Units: Researcher
Number of R&D researchers available in the company

Sales Gap=
(Actual Sales-Expected Sales)/Expected Sales
Units: USD/Month
Sales gap as the difference between expected and actual sales levels

Target Demand=
Cobb Constant*(Exclusive IP^Alpha)*(5000^(1-Alpha))+
Marketing Promotion*Marketing Factor
Units: USD/Month
Expected demand as a result of the marketing and the exclusive IP

11.6 Scientific Papers

Five of the papers that were developed during the thesis project are shared in this section to convey the extent of the work carried out during the PhD project. The aim of these papers was to engage with the relevant communities during the research process by sharing the current state of the project's research.

Paper 1 (P1) is a journal paper titled "*Supply chain cyber-resilience: creating an agenda for future research*", and it contains the first results of a structured literature review in 2015 to evaluate the applicability of resilience frameworks to cyber-risks. This review is later updated and expanded in Chapter 0 of the thesis to contain articles up to 2017 and to evaluate specifically cyber-resilience frameworks.

Paper 2 (P2) is a journal paper titled "*An endogenous exposure calculation method for cyber-risk assessment in supply chains*", and it contains the results of the application of a modified STPA method as presented in section 5.2 of this thesis, explaining the process of endogenous exposure calculation.

Paper 3 (P3) is a conference paper titled "*Extending supply chain risk and resilience frameworks to manage cyber risk*", and it contains the results of initial research into the use of systems thinking for understanding cyber-risk, both from the point of view

of causal analysis as later developed in section 6.4 of this thesis, and the dynamic simulation of behaviour, theme identified in the SLR (section 2.9.2).

Paper 4 (P4) is a conference paper titled "*Control structures in supply chains as a way to manage unpredictable cyber-risks*" and contains the partial results of research about the use of control structures, applied in this thesis both for the case of systemic risk analysis (see section 5.2) and dynamic modelling (see section 6.5).

Paper 5 (P5) is a conference paper titled "*A system dynamics case study of resilient response to IP theft from a cyber-attack*" and contains the partial results of a case study, shown in detail in Chapter 0 of this thesis.

11.6.1 Paper 1

Technology Innovation Management Review April 2015

Supply Chain Cyber-Resilience: Creating an Agenda for Future Research

Omera Khan and Daniel A. Sepúlveda Estay

> *"Resilience is all about being able to overcome the unexpected. Sustainability is about survival. The goal of resilience is to thrive."*
>
> Jamais Cascio
> Writer and futurist specializing in design strategies

Supply chains have become more vulnerable in recent years, and high-profile cyber-attacks that have crippled the supply chains of well-known companies reveal that the point of entry for hackers is often through the weakest link in the chain. Exacerbated by growing complexity and the need to be visible, these supply chains share vital streams of information every minute of the day, thereby becoming an easy and highly lucrative target for talented criminals, causing financial losses as well as damaging brand reputation and value. Companies must therefore invest in supply chain capabilities to withstand cyber-attacks (i.e., cyber-resilience) in order to guard against potential threats. They must also embrace the reality that this often-unknown dimension of risk is the "new normal". Although interest on this topic has grown in the business world, less has been reported by the academic community. One reason for this could be due to the convergence of two different disciplines, information technology and supply chains, where supply chain cyber-risk and cyber-resilience appear to have a natural fit. The topic of cyber-resilience in supply chains is still in early stages of development, and this is one of the first journals to focus a special issue on it. Currently, the closest academic literature is within the realms of supply chain risk and resilience, where numerous models and frameworks exist. In this article, this literature is explored to identify whether these models can incorporate the dimension of cyber-risk and cyber-resilience. In doing so, we create a research agenda for supply chain cyber-resilience and provide recommendations for both academia and practice.

Introduction

Supply chain management has become dependent on electronic systems; since the 2000s, we have seen the emergence of information technology solutions to support business operations, to share information, to connect businesses, and to generate greater visibility along supply chains in order to gain knowledge and control of processes. On the other hand, although supply chains have pursued aspects such as the standardization of business processes, increased communication, connectivity, and data exchange, the vulnerability of these systems to cyber-attacks is nevertheless increasing. Why is this? In modern supply chains, information is shared digitally more than any other way, and supply chains are so reliant on good quality information that, without it, supply chain managers cannot make decisions on forecasts, production, distribution, etc. Equally importantly, poor data leads to poor decisions and performance. So, even with the most efficient and responsive supply chain, performance will be greatly compromised without good quality information.

For supply chains to thrive, managers must recognize that cyber-attacks are becoming common occurrences and that the "new normal" operating environment is one that is increasingly impacted by unknown risks. A key lesson for supply chain managers is that cyber-attacks do not always "come through the front door"; a business can be greatly impacted by an attack on the weakest link in their supply chain. A key difficulty with cyber-attacks is that often a business will not know the

Technology Innovation Management Review April 2015

Supply Chain Cyber-Resilience: Creating an Agenda for Future Research

Omera Khan and Daniel A. Sepúlveda Estay

types of cyber-risks to which it has exposure, until it realizes that it is being attacked. Therefore, businesses must develop cyber-resilience to protect their supply chains.

Cyber-attacks can cause considerable economic costs to the companies that suffer these breaches, although the costs may not be noticed until after the damage is done. Estimates of the annual costs from cyber-crimes range from $375 billion to $575 billion (USD) (Intel Security, 2014), with significant effects on supply chains and resulting business performance with customers. Missing or erroneous data and information in supply chains, as a result of cyber-attacks, can lead to undesirable effects as diverse as intellectual property breaches, sub-standard or interrupted operations, sensitive data custody breaches, and decreases in service level to final customers. For example, some estimates indicate annual losses of £9.2bn from the theft of intellectual property and a further £7.6bn from industrial espionage.

Businesses that are able to understand what data is critical, where it is, who has access to it, and who is responsible for it, as well as where potential risks are in terms of information and data in the supply chain, are those that will be able to correctly communicate these risks to the supply chain in order to implement actions to mitigate them.

However, there has been a lack of managerial action to acknowledge the relevance and impact of cyber-crime (Burnson, 2013; Deloitte, 2012, 2013). It has been stated that "only a few CEOs realize that the real cost of cyber-crime stems from delayed or lost technological innovation" (Bailey et al., 2014) and companies have likely underestimated their risk (Intel Security, 2014). This is, either by delayed decision making or by a lack of awareness, the resulting inaction is leading to higher organizational costs from cyber-crimes.

This inaction is compounded by the increasing complexity of global supply chains and the speed and connectivity of operations required by companies to stay competitive. Furthermore, the growing skill of the attackers to find novel ways of accessing crucial data (Reuters, 2012), and the limited information and tools available to manage these threats, requires organizations to be more resilient to cyber-attacks that can cripple their supply chains.

Companies can prepare for potential attacks by applying appropriate supply chain risk-management tools and techniques both to reduce the likelihood of an intrusion and to deal with any disruption should an attack be successful. Every business that depends on a supply chain needs to build in cyber-resilience. But what exactly is cyber-resilience in the context of supply chains, and how can it be incorporated into current supply chain risk-management approaches?

Cyber-risk has been defined by the Institute for Risk Management (IRM, 2015) as "any risk of financial loss, disruption or damage to the reputation of an organization from some sort of failure of its information technology systems". The ISO 27005:2008 defines information security risk as "the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization" (BSI, 2008). Both of these terms are being widely used in industry, and this article will consider these terms as equivalent.

We define supply chain cyber-resilience "as the capability of a supply chain to maintain its operational performance when faced with cyber-risk".

In light of the above challenges, the purpose of this article is to create an agenda for future research that could help supply chain and IT personnel to recognize and take a proactive team-based approach to supply chain cyber-resilience. More specifically, the aims of this study are to:

1. Explore current supply chain risk and resilience frameworks
2. Analyze these frameworks and determine whether they incorporate cyber-risk
3. Create a research agenda for cyber-risk and cyber-resilience.

The remainder of this article is structured as follows. First, the process used to find and review the key literature is explained. Next, the main findings of the literature review are discussed. Finally, a research agenda for supply chain cyber-resilience is proposed, including recommendations for both academia and industry.

Methodology

A systematic literature review was conducted, based on documented guidelines (Tranfield et al., 2003) through which a comprehensive, explicit, and reproducible method is followed. This method consists of ten steps that can be grouped into five main phases:

Supply Chain Cyber-Resilience: Creating an Agenda for Future Research

Omera Khan and Daniel A. Sepúlveda Estay

1. **Planning:** The planning phase focused on defining a review question to guide the search: "Do the current supply chain risk and resilience frameworks incorporate cyber-risk?"

2. **Searching:** The searching phase was guided by the identification of the relevant databases where the search was to be done, the keywords to be used during these searches, and the appropriate timeframe for the resulting documents to be included in the research. We searched for literature using the following databases: Scopus, Web of Science, ProQuest, and Google Scholar. The search keywords were determined from a knowledge domain analysis around the concept of cyber-resilience for the supply chain (see Figure 1). The three main knowledge domains to be scanned were identified as "supply chain management", "information technology management", and "risk (& resilience) management".

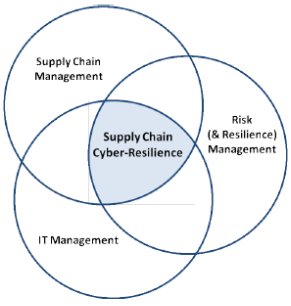

Figure 1. Main knowledge domains in supply chain cyber-risk management

3. **Screening:** After the initial, broad literature search was carried out, we conducted a preliminary analysis of the document titles and abstracts, if available. This step was followed by a more detailed analysis of the document abstracts, in the case of papers, and extended content in other cases. We applied explicit inclusion and exclusion criteria (e.g., document type, themes covered, research approaches) to identify a refined selection of documents for this analysis. Finally, the references of this refined set of articles were reviewed to identify relevant documents that might not have been identified through our initial broad search. Our final list consisted of 213 documents (24 articles, 137 peer-reviewed journal papers, 51 reports by specialized agencies, and 1 thesis). The documents covered the areas of supply chain risk management (131 documents), supply chain cyber-risk management (SCCRM), and information technology risk management (44 documents), ranging from the years 1998 to 2015.

4. **Extracting and synthesizing:** The documents were analyzed and synthesized using a spreadsheet format that allowed us to categorize the documents according to methodological approaches, contexts, outcomes, etc.

5. **Reporting:** In the next section, we report on our findings from the literature review.

Findings

Some of the earliest evidence of supply chain resilience can be found in the work of Christopher and Peck (2004), which was derived from earlier research on supply chain agility as a way of counteracting for uncertainty in the demand (Christopher & Towill, 2001), This perspective emerged after the foot-and-mouth disease event in the United Kingdom and the 9/11 terrorist attacks in United States, both of which occurred in 2001. Christopher and Peck proposed a reference model for the characterization of resilience in the supply chain, and the main aspects contributing to supply chain resilience were identified as re-engineering, organizational culture, agility, and collaboration.

Sheffi and Rice (2005) presented a disruption model based a proposed disruption theory for production systems (Asbjornslett, 1999), where this model was represented as a transient decrease in process performance. The Sheffi and Rice model identified eight sequential phases describing a disruption event: preparation, disruptive event, first response, initial impact, time of full impact, preparation for recovery, recovery, and long-term impact. Based on this model, Sheffi and Rice propose an enterprise "vulnerability map" through which the different disruption event probabilities and consequences are compared and ranked for prioritization.

Sheffi and Rice (2005) also identified product demand as the main source of uncertainty in the supply chain and acknowledged the increase in global uncertainty due to increased customer expectations, more global competition, longer and more complex supply chains, greater product variety, and shorter product lifecycles.

Supply Chain Cyber-Resilience: Creating an Agenda for Future Research

Omera Khan and Daniel A. Sepúlveda Estay

They considered organizational resilience as a strategic initiative to reduce vulnerability and therefore reduce the likelihood of occurrence of a disruption. Finally, they identified three important factors for building resiliency in an organization: redundancy, flexibility, and cultural change.

A number of other resilience frameworks have been suggested in literature. Linkov and colleagues (2013) proposed a resilience matrix of four steps representing a process for the event management cycles of disruptions: i) plan/prepare, ii) absorb, iii) recover, and iv) adapt. Each of these steps are described for different domains within the organization (i.e., physical, information, cognitive, and social). These authors have further suggested how to measure resilience according to this matrix.

Based on the framework proposed by Christopher and Peck (2004) as well as an empirical research study to identify vulnerabilities and capabilities within organizations, Pettit, Fiskel, and Croxton (2010) proposed the supply chain resiliency assessment and management (SCRAM) framework. This framework identifies an active relationship between the capabilities and the vulnerabilities in an organization, and its resulting resilience. They argue that the level of resilience that a company has to aim for is a balance between developing too many vulnerabilities (due to a lack of investment in capabilities), which could result in disruptions with undesirable economic effects, and investing in too many capabilities, which would erode profitability. Hence, they highlight an economic tradeoff between investment (capabilities) and risk (vulnerabilities).

Blackhurst, Dunn, and Craighead (2011) proposed a global resiliency framework based on systems theory and the framework proposed by Sheffi and Rice (2005). They distinguish between "resilience enhancers" and "resilience reducers", which are organizational attributes that either increase or decrease the ability of a firm to recover quickly and efficiently from a disruptive event. They identified 13 resilience enhancers and seven resilience reducers, each within three categories. Their work derives these attributes from an industrial setting and therefore can serve as basis for further research in the empirical confirmation of these or other resilience attributes.

The World Economic Forum (WEF, 2013) presented a resilience framework as part of its Supply Chain Risk Initiative. This framework attempts to quantify the risk to an organization's physical and intangible assets through a combination of effects from the existing risks to the organization and its vulnerabilities. The World Economic Forum's (WEF, 2013) resilience report also provides four recommendations for organizations to build resilient supply chains: i) put in place strong policies for the creation and adoption of resilience standards; ii) develop agile and adaptable strategies in organizations; iii) use data-sharing platforms for risk identification and response; and iv) enter into partnerships that involve all stakeholders in the risk assessment process.

Cyber-risks within the supply chain resilience framework

Our literature review did not find any supply chain resilience framework that incorporated the phenomenon of cyber-risk or information risk explicitly. However, our analysis revealed that the most influential sources for the development of cyber-resilience policy are the insurance industry, governmental requirements, and international organizations such as the World Economic Forum.

In 2012, the World Economic Forum created an initiative called "Partnering for Cyber-Resilience", led by Elena Kvochko, as a response to the increasing importance of cybersecurity. With more than 100 organizations involved, this initiative has created a series of reports describing principles for cybersecurity, recognizing interdependence, leadership, integrated risk management, and uptake by partners in the supply chain, as crucial aspects for resilience building. Additionally Kvochko has recently published an initial framework for the measurement of cyber-threats, through the calculation of a cyber-risk value and by combining eight factors grouped in three categories: vulnerability, assets, and attacker profile (WEF, 2015).

At a government level, there are several initiatives in place concerning cyber-risk and cybersecurity. In 2003, the United States government published the "National Strategy to Secure Cyberspace" (White House, 2003), and as part of a wider strategy from the Department of Homeland Security as a response to the 9/11 terrorist attacks and in line with Presidential Directive 63, which provides a framework for the protection of critical infrastructure (White House, 1998). In 2005, Germany started the "National Plan for Information Infrastructure Protection", with its main objectives being prevention, preparedness, and sustainability of the information infrastructure through the setting of international standards (German Federal Ministry of the Interior, 2005). By 2015, all EU member states except Portugal had published national cybersecurity strategies, with Estonia

Supply Chain Cyber-Resilience: Creating an Agenda for Future Research

Omera Khan and Daniel A. Sepúlveda Estay

having been the first in 2008 (ENISA, 2015; Keegan, 2014). In 2013, the United States government released Presidential Policy 21 and Executive Order 13636 to focus national attention on cyber-infrastructure resilience. In particular, Executive Order 13636 establishes a risk-based standard to protect critical infrastructure against cyber-threats. However, standards based on risk assessment do not necessarily create resilience (Linkov et al., 2013).

Conclusions and Recommendations

Our systematic literature review highlights that there is limited literature and no specific frameworks for cyber resilience in the supply chain, despite the increasing importance of the topic. The main supply chain resilience theories were proposed in the early 2000s, and the main advancements to those theories have been through the empirical identification of organizational attributes that increase or decrease resilience, as well as theoretical relationships between organizational vulnerabilities and capabilities as related to resilience. Additionally, we found that the existing supply chain resilience frameworks could be extended to consider cyber-risks through aspects such as cultural change (Sheffi & Rice, 2005) or collaboration and organizational culture (Christopher & Peck, 2004). Cyber resilience theory can also be advanced through the empirical quantification of the cyber-resilience of an organization, through case studies and stress testing of organizations with techniques such as non-invasive games (Gerencser et al., 2003).

A key contribution of this article is a definition for supply chain cyber-resilience: "the capability of a supply chain to maintain its operational performance when faced with cyber-risk". Furthermore, as a result of this study, we offer the following recommendations for academia with the goal of developing a future research agenda for supply chain cyber-resilience:

1. **Develop theory to demystify cyber-risk and cyber-resilience in supply chains:** Academics should conduct in-depth (systematic) literature reviews that confirm or expand on this study to devise methods of incorporating cyber-resilience with existing frameworks in supply chain resilience and indeed develop new models and frameworks. Finally, and fundamentally, they should align supply chain thinking and personnel with information technology issues and personnel to develop a team approach to supply chain cyber-resilience.
2. **Develop applicable tools and techniques:** There is a need for models (e.g., models of dynamic behaviour, machine-learning models for real-time monitoring of performance conditions) and practitioner workbooks (e.g., to evaluate the likelihood of detection or the probability of attack), to help practitioners better manage the causes and effects of cyber-risk to the supply chain.
3. **Generate case studies:** In-depth and longitudinal case studies within different industrial sectors are required to increase our understanding of the occurrence, detection, and reaction to cyber-attacks. Such case studies will enable researchers to validate theory and conceptual frameworks and models.
4. **Investigate the different types of cyber-attacks:** Studies should examine the attack goals (e.g., data theft, data modification, data falsification), the technical nature of attacks (e.g., tools, physical or digital barriers, verification procedures, data integrity), as well as human dimensions (e.g., cyber-attacker motivation, incentives).
5. **Propose strategic ways of managing cyber risks:** For example, academia may suggest portfolio investment to hedge risk by diversifying the business structure, where different areas counterbalance the effect of cyber-attacks. Furthermore, academia may suggest establishing appropriate key performance indicators or reviewing organizational culture and leadership, which should be empowered for proactive management of supply chain cyber-resilience.

For industry, we offer the following recommendations:

1. **The search for solutions to cyber-risks must be approached in terms of distributed accountability, instead of centralized authority:** The increasingly complex supply arrangements are creating conditions for "malevolent actors to recruit, coordinate and inflict harm across the whole network" (WEF, 2012). This challenge will require companies to adjust the current paradigm of centrally controlling risk management with routine evaluation processes (Deloitte, 2012).
2. **Re-arrange resources and develop contingency plans when necessary:** Organizations that thrive are those that can quickly recognize unusual operating conditions. It is no longer possible to prepare for every possible threat scenario. Instead, organizations

Supply Chain Cyber-Resilience: Creating an Agenda for Future Research

Omera Khan and Daniel A. Sepúlveda Estay

should prepare by encouraging team members to speak up when they detect an anomaly, having strategies in place to create customized contingency plans as necessary, and using automatic detection systems (e.g., machine learning) to identify real-time suspicious variations in performance indicators. There is a need for a new level of coordination in organizations for risk management and security response. In environments with high volatility, central controls are not sufficient and "structural integration is key to addressing uncertainties" (Boyson, 2014).

3. **Include recovery costs in the cost evaluation of cyber-attacks:** Recovery costs can surpass the direct organizational losses from cyber-attacks (Ponemon, 2014). Including recovery costs in the evaluations will highlight the real economic implications of delayed action.

4. **Create a cyber-crisis team within each organization:** Such teams should be empowered to work across organizational silos.

5. **Collaborate with academic institutions:** Academics can assist companies through training programs in cyber-resilience, by introducing new tools for the evaluation of cyber-resilience, or by providing methods for the real-time monitoring of conditions (e.g., through machine-learning methods) to detect potential threats.

6. **Promote a proactive culture:** Organizations should provide incentives for early-bird alerts on anomalous operating conditions, which promote flexibility and a proactive response in the face of an unforeseen threat.

About the Authors

Omera Khan is a Full Professor of Operations Management at the Technical University of Denmark. She works with leading organizations on a range of supply chain and logistics issues and is advisor to many universities developing courses in logistics, supply chains, and operations management. She has led and conducted research projects commissioned by government agencies, research councils, and companies in supply chain resilience, responsiveness, sustainability, and the impact of product design on the supply chain. Her latest area of research focuses on cyber-risk and resilience in the supply chain. Omera is an advisor to many organizations and provides specialist consultancy in supply chain risk management. She is a highly acclaimed presenter and is regularly invited as a keynote speaker at global conferences and corporate events. She has published her research in leading journals, contributed to several book chapters, and is lead author of *Handbook for Supply Chain Risk Management: Case Studies, Effective Practices and Emerging Trends*. She founded and was Chair of the Supply Chain Risk and Resilience Research Club and the Product Design and Supply Chain Special Interest Group. She has also been a visiting professor at a number of leading business schools.

Daniel A. Sepulveda Estay is a PhD researcher at the Technical University of Denmark, where he researches cyber-risk and security in the global supply chain. He has worked in the engineering and supply divisions of a number of multinational companies, both in strategic/leadership and operational roles for over 11 years, having partially led initiatives such as the implementation of lean manufacturing in Coca-Cola Company Latin America and supply rationalization in BHP Billiton´s copper projects division. Daniel has a BSc in Mechanical Engineering from the Federico Santa Maria Technical University in Valparaiso, Chile, an MSc degree in Industrial Engineering from the Pontifical Catholic University of Chile in Santiago, Chile, and an MSc degree in Management from the MIT Sloan School of Management, in Boston, United States.

Supply Chain Cyber-Resilience: Creating an Agenda for Future Research

Omera Khan and Daniel A. Sepúlveda Estay

References

Asbjornslett, B. E. 1999. Assess the Vulnerability of Your Production System. *Production Planning & Control*, 10(3): 219–229. http://dx.doi.org/10.1080/095372899233181

Bailey, T., Miglio, A. Del, & Richter, W. 2014. The Rising Strategic Risks of Cyberattacks. *McKinsey Quarterly*, 2 (2014): 17–22.

Blackhurst, J., Dunn, K. S., & Craighead, C. W. 2011. An Empirically Derived Framework of Global Supply Resiliency. *Journal of Business Logistics*, 32(4): 374–391. http://dx.doi.org/10.1111/j.0000-0000.2011.01032.x

Boyson, S. 2014. Cyber Supply Chain Risk Management: Revolutionizing the Strategic Control of Critical IT Systems. *Technovation*, 34(7): 342–353. http://dx.doi.org/10.1016/j.technovation.2014.02.001

BSI. 2008. *BS ISO/IEC 27001:2008 Information Technology – Security Techniques – Information Security Risk Management*. London: British Standards Institution.

Burnson, P. 2013. Supply Chain Cybersecurity: A Team Effort. *Supply Chain Management Review*, June (2013): 6–8.

Christopher, M., & Peck, H. 2004. Building the Resilient Supply Chain. *International Journal of Logistics Management*, 15(2): 1–14. http://dx.doi.org/10.1108/09574090410700275

Christopher, M., & Towill, D. 2001. An Integrated Model for the Design of Agile Supply Chains. *International Journal of Physical Distribution & Logistics Management*, 31(4): 235–246. http://dx.doi.org/10.1108/09600030110394914

Deloitte. 2012. *Aftershock: Adjusting to the New World of Risk Management*. London: Deloitte Development LLC.

Deloitte. 2013. *The Ripple Effect: How Manufacturing and Retail Executives View the Growing Challenge of Supply Chain Risk*. London: Deloitte Development LLC.

ENISA, 2015. National Cyber Security Strategies in the World. *European Union Agency for Network and Information Security*. Accessed April 1, 2015: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world

Gerencser, M., Weinberg, J., & Vincent, D. 2003. *Port Security War Game: Implications for U.S. Supply Chains*. Booz & Company.

German Federal Ministry of the Interior. 2005. *National Plan for Information Infrastructure Protection*. Berlin: Bundesministerium des Innern.

Intel Security. 2014. *Net Losses: Estimating the Global Cost of Cybercrime*. Santa Clara, CA: Intel Security

IRM. 2015. Cyber Risk and Management. *Institute for Risk Management*. Accessed April 1, 2015: https://www.theirm.org/knowledge-and-resources/thought-leadership/cyber-risk/

Keegan, C. 2014. Cyber Security in the Supply Chain: A Perspective from the Insurance Industry. *Technovation*, 34(7): 380–381. http://dx.doi.org/10.1016/j.technovation.2014.02.002

Linkov, I., Eisenberg, D. A., Bates, M. E., Chang, D., Convertino, M., Allen, J. H., Flynn, S. E., & Seager, T. P. 2013. Measurable Resilience for Actionable Policy. *Environmental Science and Technology*, 47(18): 10108–10110. http://dx.doi.org/10.1021/es403443n

Pettit, T. J., Fiksel, J., & Croxton, K. L. 2010. Ensuring Supply Chain Resilience: Development of a Conceptual Framework. *Journal of Business Logistics*, 31(1): 1–21. http://dx.doi.org/10.1002/j.2158-1592.2010.tb00125.x

Ponemon. 2014. 2014 *Global Report on the Cost of Cyber Crime*. Traverse City, MI: Penemon Institute.

Reuters. 2012. *Cyber Crime - How Can Firms Tackle This Fast-Emerging Invisible Menace?* London: Thomson Reuters.

Sheffi, Y., & Rice, J. B. 2005. A Supply Chain View of the Resilient Enterprise. *MIT Sloan Management Review*, 47(1): 41–48.

Tranfield, D., Denyer, D., & Smart, P. 2003. Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review. *British Journal of Management*, 14(3): 207–222. http://dx.doi.org/10.1111/1467-8551.00375

WEF. 2012. *Risk and Responsibility in a Hyperconnected World - Pathways to Global Cyber Resilience*. Geneva, Switzerland: World Economic Forum.

WEF. 2013. *Building Resilience in Supply Chains*. Geneva, Switzerland: World Economic Forum.

WEF. 2015. *Partnering for Cyber Resilience: Towards the Quantification of Cyber Threats*. Geneva, Switzerland: World Economic Forum.

White House. 1998. *Presidential Decision Directive NSC-63 on Critical Infrastructure Protection*. Washington, DC: The White House.

White House, 2003. *The National Strategy to Secure Cyberspace*. Washington, DC: The White House.

Citation: Khan, O., & Sepúlveda Estay, D. A. 2015. Supply Chain Cyber-Resilience: Creating an Agenda for Future Research. *Technology Innovation Management Review*, 5(4): 6–12. http://timreview.ca/article/885

Keywords: resilience, supply chain management, cyber-risk, cybersecurity, theoretical foundation

11.6.2 Paper 2

An endogenous exposure calculation method for cyber-risk assessments in supply chains

Daniel A. Sepulveda Estay

DTU Technical University of Denmark

(dasep@dtu.dk)

Omera Q. Khan, AAU

Aalborg University

Purpose

Traditional supply chain risk evaluation is based on the probability and severity of system failure modes. However, probability calculation remains largely dependent on participant experience with little reproducibility, particularly in the case of events with limited or no historical data as is the case with cyber-attacks. This paper describes a method focused on structural and context conditions that lead to unacceptable losses from cyber-attacks, irrespective of the external cause, termed "endogenous exposure". By applying this to a specific case example, the sources of greater marginal reduction of risk for effective organizational resilience building are identified and quantified.

Design / methodology / approach

The digital structure of the supply system is represented. Contexts are identified in which this structure will result in a hazardous condition that may lead to an undesirable outcome. A relative probability is calculated for each of the disruption types, as the absolute number of contexts in which a hazard and a loss can materialize.

Findings

For a two tiered supply chain, our analysis revealed 119 unsafe contexts that influenced 27 control actions leading 6 fundamental ways in which the supply chain can have an undesirable performance. The probabilities of failure due to internal structure ranged from 78% for supplier payment, to 92% for product arrival.

Originality / value

This method changes analysis focus from the external sources of risk, to the internal structures that allow risk to disrupt operations, changing the discussion from protection to capability development, and delivering concrete indications for resilience building in supply chains.

Keywords: Cyber-risks, Supply Chain Management, Resilience

Introduction

Corporate awareness of cyber risks affecting supply chains is increasing, driven by news and specialized reports that continue to uncover the existence of vulnerabilities that may be unknown until after the breach has been disruptive (Khan et al., 2015; Verizon 2016). Consequences of cyber-risks have included loss of company value through loss of intellectual property (Cashell et al., 2004; Manuj et al., 2008), and unwanted interruptions in the expected physical flow of goods and services to the supply network. The economic consequences of disruptions resulting from these cyber-risk-related vulnerabilities have been valued at US 300 billion in losses (Verizon, 2016) and not surprisingly, cyber-attacks have been identified as one of the most important risks in the supply chain (WEF, 2013).

An expectation that cyber-attacks will cause by 2030 more damage in supply chains than physical attacks (Markmann et al., 2013), is driving a steady rise in the relative importance given not only to the capacity of protecting supply systems from cyber-attacks, but also to the capacity of reacting efficiently after a cyber-attacks is declared, to minimize losses, i.e., cyber-resilience.

Supply chain's dependence on information technology (IT) has partially driven an increase in their complexity, the increasing number of people and digital systems that interact with one another, the number of interactions over time, the volume and speed at which data is being produced and exchanged, and consequently the number of ways in which operations can be disturbed. Additionally, since IT systems cannot be tested thoroughly for removal of errors before being used in operations, the digitalization of important areas of supply chain operations is both resulting in more productive, yet also more vulnerable supply systems.

By understanding supply chains as physical operations based and dependent on an underlying structure of coordinating information flows (Forrester, 1961; Sahin et al., 2002), the driver of operational disruption resides in the structure of interactions between physical systems, human operators, and IT (Baheti et al., 2011; Behdani ey al., 2012; Kull et al., 2013), including human variability (Reason, 2000).

Understanding and managing operational disruptions derived from cyber-risks is fundamental to supply chains for at least two reasons. First, correct information sharing is often considered central for efficient supply chain response (Forrester, 1961; Simchi-Levi et al, 2000; Chen et al, 2000; Sahin et al, 2002; ; Lee et al, 2004). Second, being able to maintain operations through cyber-attacks is becoming a defining characteristic of competitive supply chains (Cashell et al., 2004; Rajkumar et al.,2010; Guariniello et al, 2014; Khan et al., 2015).

Additionally, the steady increase in cyber-attack number and modes (Wood et al., 2016; Verizon, 2016), are indications of shortcomings in current methods for preparing and reacting to these attacks. This is compounded by possible under-representation of the threat due to strong incentives for companies to conceal information about cyber-attacks (Cashell et al., 2004; WEF, 2013).

In cases where the source for these disturbances is the incorrect operation or functioning of a component, traditional risk assessment tools have been effective, as probabilities of failure can be obtained from historical evidence, and the relative simplicity of the systems under analysis makes a linear causality framework applicable. However, these tools have increasingly questionable applicability in the case of events with little historical evidence and where the systems have higher complexity. Traditional methods become impractical to implement in the assessment of disruptions from cyber-attacks because of the great complexity if IT systems and interactions, their voluminous reporting, the exclusion of human judgment from the risk analysis, and their use of probabilities despite risk decisions rarely being made with quantifiable information, for example (Khan et al., 2007).

As a bridge to these gaps, this paper explores the use of a systemic risk analysis tool to understand and manage cyber risks. The contribution of this paper is thus threefold. First, this work discusses the particular nature of cyber risks when compared to physical risks. Second, from this different nature, this paper summarizes some of the gaps traditional risk assessment tools present when applied to the management of cyber-risks in supply chains. Finally, this paper describes the use of a particular systemic risk analysis tool, analyzes how this approach concentrates on the structure as both the source of disruptions and the focus of its solutions, and it justifies how this approach results in a complementary way of looking at risk and what supply chains can do about it.

The paper is structured as follows: the next section will present the theoretical background underlying this work. Thereafter this paper outlines the hypotheses guiding the research, and describes the research methodology. Finally, this work describes and discusses the results, and outlines derived areas of potential research.

Supply chain risk as an endogenous feature

From early on, risk was seen as both resulting from the influence of external conditions, and from the internal structures of the system, with a focus of maintaining the function of the system. Heckmann et al., (2015) traces the meaning of risk to the Greek navigation term "rhizikon" to reflect the need to avoid difficulties at sea, which in the early Italian trading circles was considered as the situation where ships would be lost at sea. Heckman goes on to trace this notion of danger both to external reasons such as weather or pirates, yet at the same time proposed the underlying business structure as a source of the risk: by owning one ship only, a merchant would be more exposed to fail if something happened to it, making this merchant was more vulnerable. Merchants could address diversification of risk through structural options such as owning more than one ship, for example, influencing their vulnerability levels.

Supply chain structure is not limited to physical infrastructure, but considers all information flows and storage in the system, and any resulting collaboration. Therefore, the informational structure influences the vulnerability levels in the supply chain, as can be exemplified by the iconic example of Nokia and Ericsson case. When faced with the same unexpected incident in a key supplier (Norman et al., 2004), different supply chain structures led to very different outcomes, derived from what can be said to constitute levels of internal or "endogenous" risk.

Risk has also been understood as the probability of external events that lead to a loss. This view of probabilities focuses on external events and how likely they are to occur, and has come to dominate the modern concept of business risk. This is particularly evident and extreme in supply chain risk management, where the probabilities of flooding, earthquakes and tsunamis are a regular part of the risk assessment procedures. Such approaches are challenged when unforeseeable events happen such as the ash cloud over European airspace, event which was probably missed by many of the by then existent supply chain risk assessments.

March et al., (1987) defined risk as "variation in the distribution of possible supply chain outcomes, their likelihood and their subjective values". Their definition is purely probabilistic, as the result of a decision alternative, without exploring the supply chain structure that led to that result. The organization, and in particular the supply chain, is the equivalent of a black box that reacts to decisions, and by finding the right decision, the desired outcome would be obtained.

Another external risk source approach relates to external threats and the inability of a company to cope with the consequences of this threat. Zsidizin (2003) derives a definition of supply risk by reviewing existing scientific and industrial supply risk definitions, finally proposing risk as the probability of an incident associated with inbound supply from individual supplier failures or the supply market occurring, in which its outcomes result in the inability of the purchasing firm to meet customer demand or cause threats to customer life and safety. This definition considers the risk as coming from external sources, either the supplier or the market. The purchasing firm is seen as the receiver of this risk, not its generator.

Juttner et al., (2003) defined risk as the possibility and effect of mismatch between supply and demand, which was then later expanded by Peck (2006) to any disruption of the information, material or product flows from original suppliers to the delivery of the final product to the ultimate end-user. This definition does not explore the sources if theses disruptions, and in this sense can be regarded as more general by focusing on the undesirable outcome for defining what is supply chain risk. Additionally, Peck makes the relevant contribution of singling out information, material or product flow as what can be disrupted, opening up the discussion around how these information flows can affect operations in the supply chain.

Rao et al, (2009) proposed typologies for supply chain risks, particularly environmental factors, industry factors, organizational factors, problem-specific factors, and decision-maker factors, however, the focus of the analysis is external and not systemic. Fahimnia et al., (2015) identified from literature different methods for quantifying supply chain risk, deriving seven main "generative" clusters which are those that have "…provided the field with various foundational knowledge, concepts, theories, tools and techniques…". Of these, only one cluster considered dynamic modeling, namely a cluster denominated "Information sharing: supply chain coordination, bullwhip effect, dynamic modeling" (Fahimnia et al., 2015). Moreover, when analyzing the individual papers of supply chain risk modeling and quantification, they were related to stochastic modeling and state comparison (You et al., 2008; Santoso et al., 2005; Gupta et al, 2003), equilibrium under network models (Tsiakis et al, 2001); of fuzzy sets (Petrovic et al., 1998), none of these are truly "dynamic models" as they neither explain the development of a behavior (rather concentrating on a final state), nor identify structures that lead to this behavior, thus considering "black boxes" as generators of the change. Of the models that were dynamic in nature, these concentrated on specific phenomena such as the bullwhip effect (Wangphanich et al., 2010; Moyaux et al., 2007)

Systemic-risk-analysis methods

All risk analysis methods to some extent relate to a more generic process of identifying, quantifying and reducing risk (Frosdick, 1997; Khan et al., 2007). Traditional approaches follow the analytical method of separating the problem into smaller subunits, understanding the behavior of each unit separately and then integrating this understanding into an understanding of the whole. In contrast, a systemic approach is based on a different set of ideas which characterize systems: emergence, hierarchy, communication and control. These concepts introduce ideas about coordination failure through system flaws, this is, undesirable results because of how the system was designed, not because of defective operation of any specific part of the system. This coordination flaws are particularly evident when looking at information flows.

Forrester from the Massachusetts Institute of Technology (MIT) developed in the 1960's a theory for "…the study of information feedback characteristics of industrial activity to show how organizational structure, amplification (in policies), and time delays (in decisions and actions) interact to influence the success of the enterprise" (Forrester 1961, p. 13), laying the foundation for our current understanding of coordination in supply chains. This development was

based on control theory applied to organizations, identifying feedback loops as the structures that drive dynamic supply chain behavior.

Feedback loops are constructs of circular causality composed of flows and accumulations. The different accumulations will have incoming and outgoing flows, and are the result of the sum of these flows over time (integration). System dynamics postulates that it is the decisions (policies) on the different inflows and outflows that give rise to the dynamic behavior in a system. Feedback loops have been identified as the sources of dynamic behavior in complex systems from of at least six intellectual traditions: engineering, economics, biology, mathematical models of biological and social systems, formal logic, and classical social science (Richardson, 1999).

A systemic approach to risk management was suggested by White (1995) as a synthesis from a study of existing risk assessment methods, suggestion driven by both the increasing number of hazards and failures that accompany the adoption of new technologies, and the different shortcomings in existing methods to manage this complexity.

Carroll (1998), for the case of industries with high levels of hazard, highlighted that "…a high level of complexity and the tight coupling among problems seems to require a more comprehensive [approach] than those typically employed.." suggesting that traditional solutions, although well-intentioned, fail to help through their unintended side-effects. Carroll goes on to indicate that well-intentioned commonplace solutions can actually hinder improvement, and even exacerbate the problem these intended to mitigate. He therefore proposes a problem-solving dynamic that would include both problem fixing and goal learning, as well as "…modeling tools to organize dynamic interdependencies, and feedback about effectiveness".

Kang and his team have used a systems approach to identify Limiting Conditions for Operation (LCOs) in operations, extensible to supply chains (Kang et al., 2005). Their approach acknowledges three important aspects: 1) a system dynamics approach ensures a causal relationship in the establishment of the feedback loop structure, 2) the approach is useful for understanding the behavior of a complex system over time, and 3) a systemic approach is useful in conceptualizing a thorough understanding of human interactions within complex systems. Although Kang uses a system approach for modeling the system, the feedback loops structures are not mentioned, and several of the relationships are expressed in probabilistic terms.

More recently, Ghadge et al.,(2013) proposed a systemic approach based on three pillars of risk analysis: risk identification, risk assessment and risk mitigation. Through the generation of a system dynamics model containing different attributes and parameters, risks can be simulated and sensitivity analyses can be obtained on the relevance of each parameter. However, although the results and simulation clearly point out to a system dynamics model, it is unclear what feedback loops, delays and sources of inertia, i.e., stocks (Sterman, 2000) were considered.

Garbolino et al. (2016) and his team have used system dynamics modeling and risk analysis to propose a dynamic risk analysis method that includes both constraints and dynamics. Their modeling approach focuses on the strengthening of constraints, and it considers a dynamic process where industrial systems continually adapt to external and internal changes to achieve their goals. The model proposes a ten-step approach that results in scenario analysis. It is however restricted to a single plant and its internal process, thereby lacking the integration with other supply chain partners.

Our research process did not find documented literature on the application of systemic risk analysis methods such as STPA in supply chains or to cyber-risks. However, several characteristics of cyber-risks in supply chains make the STPA methodology adequate for analyzing these risks. These reasons are outlined in Table 1.

Table 1: Traditional risk assessment methods versus STPA

Characteristics of Cyber attacks	Traditional Methods Inadequacy (Chain of Events)	STPA Methodology characteristics
Occur in complex networks of information storage and exchange	Traditional methods do not represent networked relationships, rather modes of failure in the components of the network. Connections, if present, are hidden in the descriptions of the failure modes.	Considers systems as a network of interrelated components.
Occur in a great variety of different ways	Traditional methods rely on an exhaustive enumeration of the modes in which an accident can occur. This is impractical for complex networks due to the number of potential failure modes.	STAMP is based on a hierarchy of control, therefore complex problems can be decomposed or aggregated according to the required level of analysis complexity.
Management emphasis during cyber-attacks is on the recovery process (Resilience)	Traditional Methods do not describe evolution over time of the system, and are static descriptions of the system	STAMP is based on a Feedback control mechanisms of information and control, and thus behavior evolution over time is a central characteristic of this model structure

Methodology

The methodology used in this paper is an adaptation of a systemic risk analysis framework known as STPA (Systems-theoretic process analysis) developed by Leveson (2011) and her team at the Massachusetts Institute of Technology. This paper adapts STPA to consider the nature of cyber risks in a supply chain and their effect on the information flow and storage and thus on physical operations.

STPA belongs to the general family of failure tree analyses, as it starts from the identification of undesirable outcomes, or "acceptable losses", yet in contrast to the classic failure tree analysis, STPA adopts a meta-causal approach: instead of looking at individual actions that lead to undesirable outcomes, STPA considers the systemic situations that lead to these losses- called hazards- to then identify the conditions in which the actions already designed into the system - known as control actions - can lead to these hazards and thus to the losses that want to be avoided.

STPA assumes an internal source of risks - endogenous view of causality - by understanding failure as a result of the structure of the system, and not due to external factors of the disruption. This is a model based on systems theory rather than traditional analytic reduction and reliability theory. According to the systemic view, design considerations for the system (or the lack of these) are the causes of an undesired outcome. It is thus a complementary approach to protection from external threats, by focusing on protecting the system "from its own design". A safe operation is seen as an emergent property resulting from the interactions between the system components and with the environment. The problem of avoiding "accidents" (i.e., unplanned loss events) thus becomes a dynamic control problem of limiting the ways in which the system can behave by designing the structure underlying this behavior.

From this perspective, cyber-attacks are not merely events that happen to supply chains, but rather events which supply chains are "misdesigned" to experience. Cyber-attacks are thus unintended consequences (Sterman, 2001) that result from incomplete requirements (Leveson, 2011) at the time of supply chain design, and that are reflected in a structure that allows these attacks to occur. A systemic analysis seeks to identify this "unrequested" design that results in cyber-vulnerability, and determine structural changes through which a cyber-vulnerable behavior is less likely to occur or no longer possible.

Literature has been published about the description of the STAMP methodology framework (Estefan, 2007; Leveson, 2011; Salmon et al., 2012; Altabbakh et al., 2013), with examples of application in several domains, such as medical industry (Antoine,2013), environmental studies (Hardy et al., 2011), robotics (Mitka et al., 2015), power production

(Karami et al., 2015), software development (Wang et al., 2016), aerospace (Ishimatsu et al., 2014) and defense (Chiesi, 2016). No application has been documented however for supply chains or cyber risks in supply chains.

Figure 1 shows the STPA application to cyber-risks in supply chains as proposed by this paper.

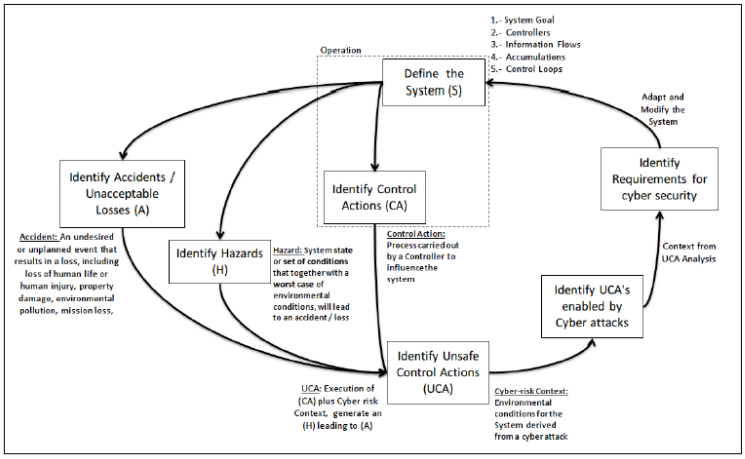

Figure 1 Modified STPA Process as applied to cyber-risk assessment (based on Leveson, 2011)

Results

Case study

The case company is a beverage manufacturer based in the US with manufacturing operations in 23 countries. This company has a complex supply chain and has a distributed, global supply team that procures raw materials and packaging to all operations through a regional structure. As a result, every world region has a relationship with local suppliers in the case of packaging, and global suppliers for the case of raw materials. Global suppliers are managed centrally in the US headquarters, while regional supply manages daily operations with these suppliers. This company is particularly interested in understanding the exposure they have to cyber-risks, as they are very sensitive to public opinion and reaction in the case they were to be attacked.

According to the systems engineering approach, we start by identifying a system goal to be achieved, which in the case of the case company it had been defined as:

A typical purchase transaction consists of a set of interactions between a buyer and a seller for the timely delivery of a product at the agreed price to the buyer through the use of a transport agent. The process begins when the buyer sends a purchase order to the seller, and ends when all involved have been paid and the product has been delivered. Process steps have been indicated in Table 2.

From the process diagram, the controllers and control actions are identified through a controller identification matrix and represented through a hierarchical control structure, and are used for different ends. The controller identification matrix is a way of identifying explicitly all existing controllers and control actions for the required processes, and it can easily highlight when either are missing. Table 2 shows the matrix for this case study.

Table 2 Controller and control action identification matrix

	Control Actions	Controllers				
		Plant	Supplier	Transport	Plant's Bank	Supplier's Bank
Process Steps	Order	*Activate Purchase Order *Cancel purchase order	*Confirm purchase order *Confirm purchase order cancellation	-	-	-
	Prepare	-	*Activate service order *Cancel service order	*Confirm service order activation *Confirm service order cancellation	-	-
	Outbound Check	-	*Handover products to transport *Handover transport documents to transport	*Perform outbound check	-	-
	Pickup	-	-	*Perform pickup	-	-
	Transport	-	*Send documentation	*Perform delivery	-	-
	Inbound Check	*Perform inbound check	-	-	-	-
	Receive	*Receive product	-	-	-	-
	Validate	*Validate product	-	-	-	-
	Pay	*Order supplier payment *Cancel supplier payment	*Order transport payment *Cancel transport payment	-	*Confirm supplier payment order *Confirm supplier payment order cancellation *Transfer funds to supplier	*Confirm transport payment order *Confirm transport payment order cancellation *Transfer funds to transport

On the other hand, the hierarchical control structure is aimed at showing the structure of the controllers and their degree of control. The higher up these are located in the diagram, the higher their hierarchy as represented in their ability to determine the objectives of the system and to control the activity of those controllers located below them in the diagram. Figure 2 shows the hierarchical control structure diagram for this case study.

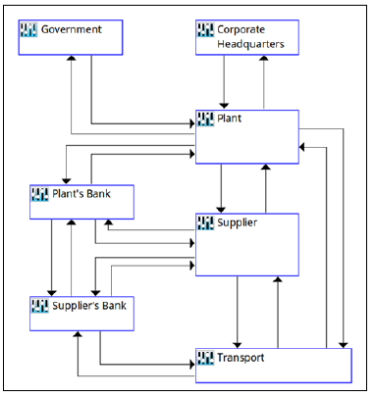

Figure 2 - Hierarchical control structure

Analysis of Hazards through unsafe control actions

For the case study supply chain, the accidents or unacceptable losses were defined by a team of experienced supply chain practitioners (Ford et al., 1998) from the case company. These unacceptable losses are directly related to the functions that management wants to maintain, objectives of this supply system, and the result of the analysis is therefore directly relevant to the objectives of these stakeholders. This list is shown in Table 3.

Table 3: Unacceptable accidents /losses in the supply chain

A1	Erroneous arrival of product
A2	Erroneous payment to supplier
A3	Product loss
A4	Product integrity compromised
A5	Payment Loss
A6	Reputational Loss

The hazards present in the system that are derived from the unacceptable accidents are shown in Table 4.

Table 4: Hazards in the supply chain

H1	Inability to initiate supply process
H2	Inability to perform physical transport
H3	Inability to confirm product integrity
H4	Inability to confirm correct payment
H5	Inability to confirm data integrity
H6	Inability to confirm data transmission integrity

As indicated in the methodology, unsafe control actions were then identified through the contexts that would then lead to an accident causing hazard. Table 5 shows an extract of the information that was obtained.

Table 5: Extract of UCA information

Control Action	CA Description	Source	Destination	UCA
1	Confirm payment order	Plant's Bank	Plant	Not providing Order Payment Confirmation when there has been a supplier payment order is hazardous
1	Confirm payment order	Plant's Bank	Plant	Providing Order Payment Confirmation when there has not been a supplier payment order is hazardous
1	Confirm payment order	Plant's Bank	Plant	Providing Order Payment Confirmation before there has been a supplier payment order is hazardous
3	Order Supplier payment	Plant	Plant's Bank	Not providing Supplier Payment Order when there has been confirmation of product reception and validation is hazardous
3	Order Supplier payment	Plant	Plant's Bank	Providing Supplier Payment Order when there has not been a product reception is hazardous
3	Order Supplier payment	Plant	Plant's Bank	Providing Supplier Payment Order when there has not been product validation is hazardous
3	Order Supplier payment	Plant	Plant's Bank	Providing Supplier Payment Order before there has been product reception is hazardous
3	Order Supplier payment	Plant	Plant's Bank	Providing Supplier Payment Order before there has been product validation is hazardous
3	Order Supplier payment	Plant	Plant's Bank	Providing Supplier Payment Order when there has not been a supplier payment data confirmation is hazardous
4	Cancel supplier payment	Plant	Plant's Bank	Not providing Supplier Payment Cancellation when there has not been product reception is hazardous
4	Cancel supplier payment	Plant	Plant's Bank	Providing Supplier Payment Cancellation when there has been product validation, reception and supplier data confirmation is hazardous
4	Cancel supplier payment	Plant	Plant's Bank	Not providing Supplier Payment Cancellation when there has not been product validation is hazardous
4	Cancel supplier payment	Plant	Plant's Bank	Not providing Supplier Payment Cancellation when there has not been a supplier payment data confirmation is hazardous
5	Activate Purchase Order	Plant	Supplier	Not providing Purchase Order Activation when there has been a confirmed requirement is hazardous
5	Activate Purchase Order	Plant	Supplier	Providing Purchase Order Activation when there has not been a confirmed requirement is hazardous
5	Activate Purchase Order	Plant	Supplier	Providing Purchase Order Activation before there has been a confirmed requirement is hazardous
5	Activate Purchase Order	Plant	Supplier	Providing Purchase Order Activation when the supplier has not been confirmed is hazardous

Discussion

The structured approach presented in the last section results in 119 different unsafe control actions, which is equivalent to the same number of contexts that lead to a hazard. This is a list, agreed by the members of the organization, of the different ways in which the existing design of this supply chain can result in an unwanted event. In the terminology of the method, any of these 119 "contexts" can make a "control action unsafe", leading to a "hazardous condition" that can create an "unacceptable loss".

This approach does not contradict other static frameworks for resilience (Christopher et al., 2003), and builds from the original "disruption curve" by Sheffi & Rice (Sheffi et al., 2005), expanding the theory by proposing mechanisms through which this behavior over time is achieved in a supply chain after a cyber-attack (cyber-resilience). The representation of information flows through a structured method with an explicit result, i.e., the information flow map, has been shown to enhance team productivity and effectiveness (Sterman 2000).

Despite this very great number of contexts not being a rare outcome as it has been the finding of many of the applications of this methodology to other processes, problems arise from these results that are worth mentioning. These problems are derived from the number of results, and from the nature of the results that are generated.

The number of unsafe control actions can be understood as a greater granularity of vulnerabilities present in the supply chain, yet this granularity also can be seen as adding greater complexity in the management of these risks. It is therefore unlikely that a company will directly undertake actions to mitigate all the contexts uncovered though this analysis, for reasons that range from technical to political. Technical reasons are related to resources and timing, such as insufficient available resources to address and resolve all unsafe contexts, while political reasons are related to strategy and conflicts of interest, such as the unwillingness of supply management to expose so many new risks not considered previously for fear of appearing incompetent to upper management.

The nature of the results also differs from the results in the probability/severity risk analyses. This methodology does not assign a probability to the unsafe control actions or contexts, as these are detected from current supply chain design. Therefore their probability of "occurrence" is 1: these design flaws exist in the system until these are solved or these are exploited. The only applicable probability is the one related to how likely an internal or external agent is to "make use" of any one of these contexts resulting in an accident. This calculation of external threat likelihood is beyond this method as this reasoning is not endogenous: the approach presented here is equivalent to finding after an analysis that a great number of open doors exist in a system where you do not want external entry. These doors will remain open until the organization decides to address this finding, unless the management decision is to consider the likelihood of anyone foreign actually attempting to use any one of these doors.

A way of quantifying this exposure is through the calculation of probabilities for the most likely hazards and accidents, thus providing management information to focus action on the ones with the highest number of ways in which an accident can be triggered. This calculation is based on the "database" of contexts which can also be understood as a traceable register of the different sources of probability. If there are N different contexts identified through the analysis, the probability would be calculated as the number of applicable contexts for the specific hazard over the total number of contexts:

Eq. 1 $$P(Hazard_i) = \frac{\sum_{j=1}^{N}((Context_j) \cup (Hazard_i))}{\sum_{j=1}^{N}(Context_j)}$$

A similar calculation can be made for the accidents, for the case of N different contexts and T different hazards.

Eq.2 $$P(\text{Accident}_i) = \frac{\sum_{k=1}^{T}\sum_{j=1}^{N}((\text{Context}_j) \cup (\text{Hazard}_k) \cup (\text{Accident}_i))}{\sum_{j=1}^{N}(\text{Context}_j)}$$

The results for the data from this case are shown next. Table 6 shows the number of accidents, hazards, control actions and unsafe control actions identified for this case study. Table 7 shows the number of UCA for each accident, and the probability as the proportion of the total number of potential UCAs which actually lead to the specific accident, proposed in this work as an "endogenous exposure" measure for the organization.

Table 6 – Accidents, hazards, control actions and unsafe control actions in the system

Symbol	Name	Number
ACC	Accidents	6
HAZ	Hazards	6
CA	Control Actions	27
UCA	Unsafe Control Actions	119

Table 7 – Unique UCA per Accident

Accident	CA	UCA	P(Accident)
Erroneous payment to supplier	16	93	78%
Product Integrity compromised	17	103	87%
Reputational Loss	15	92	77%
Erroneous arrival of product	18	110	92%
Product Loss	17	105	88%
Payment Loss	16	93	78%

In the same way, Table 8 shows the number of UCAs for the different hazards as defined for this case study. The probability for each is defined as the proportion of UCAs of the total that lead to the specific hazard.

Table 8 – Unique UCA per Hazard

Hazard	CA	UCA	P(Hazard)
Inability to perform physical transport	8	41	34%
Inability to initiate supply process	6	20	17%
Inability to confirm data transmission integrity	13	79	66%
Inability to confirm product integrity	10	44	37%
Inability to confirm data integrity	12	54	45%
Inability to confirm correct payment	8	33	28%

Of the types of UCA, (Leveson, 2011), 45% of the UCAs found correspond to a control action being executed in such a way that a hazard becomes possible, and four was the largest number of hazards assigned for a single UCA.

Considering the information within the supply chain as either a stock or a flow of information, our analysis presented in Table 9 proposes the categorization of the unwanted behavior (UCAs).

Table 9 - Information system requirements

SD UCA Categories	Data (Stock)	Process (Flow)	Generic Type	Behavior Description	Requirement
Normal Operation	Correct	Correct		Process within the designed behavior	No requirement
Data Corruption (Stock Problem)	Incorrect	Correct	GT1	Members of the system cannot identify each other unequivocally	Information system will include a process through which each system member can identify each other unequivocally
			GT2	Data for the process is changed without members of the system noticing	Information system will include a data management process that will detect changes in data
Flawed Process (Flow Problem)	Correct	Incorrect	GT3	Process sequence advanced before confirmations are made	Information system will support the process sequence and confirmation milestones
			GT4	Process sequence understanding is different between the members of the system	Information system will continually communicate to all system members about the process sequence
Compound Problem	Incorrect	Incorrect	GT5	Wrong data is used for the process without members noticing	Information System will include communication data confirmation as milestone before data exchange between members
			GT6	Reaction times between members are not known leading to untimely decisions	Information system will continually communicate all system members about required action dates.

Conclusions, recommendations and future work

This paper proposes and develops an approach for understanding cyber risks in supply chains as caused by the internal digital structures of the supply chain, i.e., the "endogenous sources" of cyber-risk. These digital structures are the information flows, information storage, and resulting actions by the members of the supply chain. A structured methodology is used on a case study for the identification of vulnerabilities and constraints that condition its response to a cyber-attack.

Some recommendations can be derived from this work.

- Understand the information flows in your supply chain, as these are the foundation for the physical flows that take place in the supply chain.
- Control structures involving information flows in supply chains span over different areas of the company, requiring the interaction of different departments during a cyber-attack. The outsourcing of IT can hinder the response in the face of a cyber-attack, as it both eliminates the existence of some necessary feedback loops in the supply chain, or creating conflictive interests between the outsourcing IT company and the requirements of the supply chain.
- The focus of the management of cyber-risks should also include the management of the systemic structure (requirements and constraints) as well as interactions, both high leverage options. On the other hand, static structure analysis and correcting of behavior are both low leverage strategies. Investment in firewalls or anti-virus are examples of focusing the prevention on creating limits to the access of hackers, while having no effect on the behavior of the operators who gave rise to this unauthorized access, or the conditions that gave rise to this behavior being plausible for the operator in the first place.
- The level of aggregation is highly dependent on the problem that is being solved. As is the case with all models, it is impractical to attempt to model the complete system, and the level of aggregation will be the result of an iterative process of adjustment.

- The process of hazard and requirements identification is an ongoing, cumulative process that is adjusted by new hazards as these are identified and integrated into the analysis.
- There is potential for modularization of the requirements, as similar requirements can be implemented to different suppliers.
- A systemic risk analysis as shown in this paper is highly sensitive information, and should be treated as highly strategic, as it will lay open all detected available vulnerabilities in the system, and it is very unlikely that these vulnerabilities will be addressed simultaneously.

Beyond the existing industrial incentives towards not disclosing cyber-attacks when these happen, the results shown in this paper point to several other challenges, categorized as perceptual/strategic, methodological, and industry-related.

Perceptual / strategic: The endogenous point of view causality and risk exposure, despite being theoretically and methodologically grounded, is not of easy adoption by practitioners. Traditional methods of protection either structural (e.g., firewalls, antiviruses) or financial (e.g., insurance) receive priority to capability building in the organization for effective reaction. Research is needed to understand the structural foundation behind this pattern as reasons can be multiple; as an attempt to continue outsourcing the management of these processes to external IT or insurance companies to comply with actions by others in the industry; as a response to incentives that reward short term results while capability building is medium or long term in its effects; or as a way of distancing management from the source of the vulnerabilities given that the endogenous viewpoint indicates internal decisions as the sources of the problem, for example.

Methodological: Starting from the foundation that all physical flows in the supply chain are a result of an underlying information flows, storage and derived actions, the control diagram representation can also be improved to include other aspects of dynamic behavior, such as relevant accumulation of information and delays that reflect policies in the organization. A comparison of existing methods could be attempted to suggest improvements to contribute to more effective representation of the mental models regarding information flow present in the system. This work also suggests the potential for a network representation of the information flows, and of the research of potential applications of network theory for understanding aggregate effects for these flows in the supply chain when targeted by a cyber-attack.

Industrial: The application of STPA and other systemic analysis methods can be extended to different supply chains and industries, to understand if the system requirements change with the variation of the application domain or supply chain structure. The application to ex-post examples, i.e., where a cyber-attack has occurred resulting in an operational disruption, can help understand the information flows which are more relevant at the time of coordinating a reaction to a cyber-attack in the supply chain. It is also possible to explore the quantification of the effects of different factors and their relationship to the resulting cyber-resilience of the supply chain, and performance testing under different scenarios for varying requirements and constraints.

References

Altabbakh, H., Alkazimi, M. A., Murray. S., Grantham, K., 2014. STAMP – Holistic system safety approach or just another risk model?, Journal of loss prevention in the process industries, 32, pp. 109-119.

Antoine, B., 2013. Systems Theoretic Hazard Analysis (STPA) applied to the risk review of complex systems: an example from the medical device industry (Doctoral dissertation, Massachusetts Institute of Technology).

Antonakis, J., Bendahan, S., Jacquart, P. and Lalive, R., 2014. Causality and endogeneity: Problems and solutions. The Oxford handbook of leadership and organizations, pp.93-117.

Baheti, R. and Gill, H., 2011. Cyber-physical systems. The impact of control technology, 12, pp.161-166.

Behdani, B., 2012, December. Evaluation of paradigms for modeling supply chains as complex socio-technical systems. In Proceedings of the 2012 Winter Simulation Conference (WSC) (pp. 1-15). IEEE.

Carroll, J.S., 1998. Organizational learning activities in high-hazard industries: the logics underlying self-analysis. Journal of Management studies, 35(6), pp.699-717.

Cashell, B., Jackson, W.D., Jickling, M. and Webel, B., 2004. The economic impact of cyber-attacks. Congressional Research Service Documents, CRS RL32331 (Washington DC).

Chiesi, S.S., 2016, January. STPA application for safety assessment of generic missile systems. In 2016 Annual Reliability and Maintainability Symposium (RAMS) (pp. 1-7). IEEE.

Estefan, J.A., 2007. Survey of model-based systems engineering (MBSE) methodologies. Incose MBSE Focus Group, 25(8).

Fahimnia, B., Tang, C.S., Davarzani, H. and Sarkis, J., 2015. Quantitative models for managing supply chain risks: a review. European Journal of Operational Research, 247(1), pp.1-15.
Ford, D.N. and Sterman, J.D., 1998. Expert knowledge elicitation to improve formal and mental models. System Dynamics Review, 14(4), pp.309-340.
Forrester, J., 1961. Industrial Dynamics, System Dynamics Series, Pegasus Communications.
Frosdick, M. (1997), "The techniques of risk management are insufficient in themselves",Disaster Prevention and Management, Vol. 6 No. 3, pp. 165-77
Garbolino, E., Chery, J. P., Guarnieri, F., 2016. A simplified approach to risk assessment based on system dynamics: an industrial case study, Risk Analysis (2016).
Ghadge, A., Dani, S., 2013. A systems approach for modelling supply chain risks, Supply Chain Management: An international Journal, 18(5), pp. 523-538.
Gupta, A. and Maranas, C.D., 2003. Managing demand uncertainty in supply chain planning. Computers & Chemical Engineering, 27(8), pp.1219-1227.
Hardy, K. and Guarnieri, F., 2011, May. Modelling and hazard analysis for contaminated sediments using stamp model. In 14th International Conference on Process Integration, Modelling and Optimisation for Energy, Saving and Pollution Reduction (Vol. 25, pp. 737-742).
Heckmann, I., Comes, T. and Nickel, S., 2015. A critical review on supply chain risk–Definition, measure and modeling. Omega, 52, pp.119-132.
Ishimatsu, T., Leveson, N.G., Thomas, J.P., Fleming, C.H., Katahira, M., Miyamoto, Y., Ujiie, R., Nakao, H. and Hoshino, N., 2014. Hazard analysis of complex spacecraft using systems-theoretic process analysis. Journal of Spacecraft and Rockets, 51(2), pp.509-522.
Jüttner, U., Peck, H. and Christopher, M., 2003. Supply chain risk management: outlining an agenda for future research. International Journal of Logistics: Research and Applications, 6(4), pp.197-210.
Karami, E., Goodarzi, Z., Hosseinzadeh, T. and Shirali, G.A., 2015. Analyzing Hazards using System Theoretic process analysis (STPA) Methodology: A Case Study In The emergency extinguishing systems of Thermal power plant. Journal of Health and Safety at Work, 5(1), pp.13-24.
Kang, K. M., Jae, M, 2005. A quantitative assessment of LCOs for operations using system dynamics, Reliability Engineering and System Safety, 87, pp.211-222.
Khan, O. and Burnes, B., 2007. Risk and supply chain management: creating a research agenda. The international journal of logistics management, 18(2), pp.197-216.
Khan, O. and Estay, D.A.S., 2015. Supply Chain Cyber-Resilience: Creating an Agenda for Future Research. Technology Innovation Management Review, 5(4).
Kull, T.J., Ellis, S.C. and Narasimhan, R., 2013. Reducing Behavioral Constraints to Supplier Integration: A Socio-Technical Systems Perspective. Journal of Supply Chain Management, 49(1), pp.64-86.
Leveson, N., 2011. Engineering a safer world: Systems thinking applied to safety. MIT Press.
Manuj, I., Mentzer, J. 2008. Global supply chain management strategies, International Journal of Physical Distribution and Logistics Management, 38(3), pp. 192-223.
March, J.G. and Shapira, Z., 1987. Managerial perspectives on risk and risk taking. Management science, 33(11), pp.1404-1418.
Markmann, C., Darkow, I.L. and von der Gracht, H., 2013. A Delphi-based risk analysis—Identifying and assessing future challenges for supply chain security in a multi-stakeholder environment. Technological Forecasting and Social Change, 80(9), pp.1815-1833.
Mitka, E. and Mouroutsos, S.G., 2015. Applying the STAMP system safety engineering methodology to the design of a domestic robot. International Journal of Applied Systemic Studies, 6(1), pp.81-102.
Moyaux, T., Chaib-draa, B. and D'Amours, S., 2007. Information sharing as a coordination mechanism for reducing the bullwhip effect in a supply chain. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 37(3), pp.396-409.
Norrman, A. and Jansson, U., 2004. Ericsson's proactive supply chain risk management approach after a serious sub-supplier accident. International journal of physical distribution & logistics management, 34(5), pp.434-456.
Peck, H., 2006. Reconciling supply chain vulnerability, risk and supply chain management. International Journal of Logistics: Research and Applications, 9(2), pp.127-142.
Petrovic, D., Roy, R. and Petrovic, R., 1999. Supply chain modelling using fuzzy sets. International journal of production economics, 59(1), pp.443-453.
Reason, J., 2000. Human error: models and management. Bmj, 320(7237), pp.768-770.
Richardson, G.P., 1999. Feedback thought in social science and systems theory. Pegasus Communications, Inc..

Salmon, P.M., Cornelissen, M. and Trotter, M.J., 2012. Systems-based accident analysis methods: A comparison of Accimap, HFACS, and STAMP, Safety science, 50(4), pp.1158-1170.
Santoso, T., Ahmed, S., Goetschalckx, M. and Shapiro, A., 2005. A stochastic programming approach for supply chain network design under uncertainty. European Journal of Operational Research, 167(1), pp.96-115.
Sterman, J., 2000. Business Dynamics: Systems thinking and modeling for a complex world, Boston, Irwin/McGraw-Hill
Sterman, J.D., 2001. System dynamics modeling: tools for learning in a complex world. California management review, 43(4), pp.8-25.
Tsiakis, P., Shah, N. and Pantelides, C.C., 2001. Design of multi-echelon supply chain networks under demand uncertainty. Industrial & Engineering Chemistry Research, 40(16), pp.3585-3604.
Verizon, 2016.Data breach Investigations report (DBIR) 2016. Accessed on 08 November 2016. http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf
Wang, Y. and Wagner, S., 2016, May. Towards applying a safety analysis and verification method based on STPA to agile software development. In Proceedings of the International Workshop on Continuous Software Evolution and Delivery (pp. 5-11). ACM.
Wangphanich, P., Kara, S. and Kayis, B., 2010. Analysis of the bullwhip effect in multi-product, multi-stage supply chain systems–a simulation approach. International journal of production Research, 48(15), pp.4501-4517.
WEF, 2013. Building resilience in supply chains. Industry agenda report. Accessed in 12 November 2015 at http://www3.weforum.org/docs/WEF_RRN_MO_BuildingResilienceSupplyChains_Report_2013.pdf.
White, D., 1995. Application of systems thinking to risk management: a review of the literature. Management Decision, 33(10), pp.35-45.
You, F. and Grossmann, I.E., 2008. Design of responsive supply chains under demand uncertainty. Computers & Chemical Engineering, 32(12), pp.3090-3111.
Zsidisin, G.A., 2003. A grounded definition of supply risk. Journal of Purchasing and Supply Management, 9(5), pp.217-224.

11.6.3 Paper 3

Extending supply chain risk and resilience frameworks to manage cyber risk

Daniel Alberto Sepulveda Estay (dasep@dtu.dk)
Technical University of Denmark - DTU

Omera Khan
Technical University of Denmark - DTU

Abstract

This paper proposes two complementary tools for the description and quantification of dynamic effects arising from supply chain cyber-attacks. The first tool proposes a comprehensive analysis of the problem space through system dynamics methods, to identify explicitly mental models regarding aspects such as stakeholders, relevant relationships, feedback effects and potential policy levers. The second tool is proposed as a way of transitioning towards a dynamic analysis of the problem of cyber-attacks on supply chains, and is complementary to existing risk analysis tools.

Keywords: Supply chain, cyber-risk, resilience

Introduction

Cyber-risks are an increasingly relevant phenomenon in supply chain management enabled by an information technology-dependent, and increasingly complex supply network with ubiquitous access to technology. This is evidenced by recent cyber-attacks on organizations, targeting anywhere from their financial systems to confidential product or customer information, with potentially severe effects to reputational capital, supply operations, and production processes, to name a few. A key difficulty with cyber-attacks is that often companies will not know that they are at risk until they are being attacked.

Competitive pressures are forcing companies to be responsive, and to consider network competition where "prizes will go to those organizations that can better structure, co-ordinate and manage the relationships with their partners in a network committed to delivering superior value in the final market place" (Christopher, 2011). Supply chains are thus IT-dependent complex networks of agents in constant exchange of information, i.e., data, products and financial resources.

The two aspects crucial to executives when looking to reduce vulnerabilities are security- a preventive aspect which leads to the reduction of the likelihood of a disruption; and resilience- the organizational capabilities for returning to normal operating conditions after a disruption (Sheffi, 2005). Since cyber-attacks can potentially access and impact every company in a shared network, this system will only be as resilient as the weakest link in the supply network.

Traditional risk management theory has been based on a process of risk identification (modes of failure), risk impact evaluation, risk prioritization, preventive action toward diminishing the probability of occurrence for the risks with a priority above a certain threshold, and subsequent control that these preventive actions were executed.

However, increasing supply chain complexity is creating modes of failure in a supply chain beyond the preventive analysis capabilities of the organization. Therefore, it is becoming increasingly difficult to foresee every possible way in which a supply chain can be disrupted.

In the case of cyber-risks, this is particularly relevant, as increased dependence on IT has been reported to result in an increased number of suppliers in a network (Dederick et al., 2008) hence increasing the number of links where cyber-attacks can root and deploy to other parts of the target network.

There seems to be a consensus on what constitutes supply chain risk management (Khan et al., 2007), and considers the identification, analysis and control of those supply chain risks that could financially undermine the assets or earning capability of an organization, within the context of its overall aims. Methods have been developed to manage uncertainty in the supply chain, through coordination procedures (Sales & Operations Planning, Collaborative Planning Forecasting & Replenishment) for existing operations, and risk management (e.g., Business Continuity Planning) to detect additional procedures/capabilities required to better manage disruption events.

This work analyses the literature on supply chain resilience frameworks and cyber-attack types to analyse the application of these frameworks to cyber risks. This work then proposes two types of tools as contributions to bridging the research gap. One of the tools is intended towards a systemic description of the problem landscape for creating a research agenda, and as a tool to explicitly map the mental models (Doyle et al., 1998) of the problem at hand when used through group model building, for example. The second tool seeks to bridge the gap between current accepted practices, which themselves fall short for the adequate description and management of a dynamic problem, and which is presented as a complement to existing risk assessment tools.

Cyber-attack types

Our analysis of the literature showed that the types of cyber-attacks that can affect supply chains have been gathered from two main sources: a) the theoretical development of cyber-attack taxonomies and classifications based in information technology research (deductive method), and b) through the record and classification of attacks derived from information gathered with industrial practitioners (inductive method).

Furthermore, the analysis showed relevant contributions through the deductive approach of the description of supply chain cyber risks from the point of view of IT vulnerabilities. These categorizations are derived from a systematic assessment of IT/SC structure, are later tested against case studies, and are normally presented as peer-reviewed articles.

Gordon (Gordon et al., 2006) developed a cybercrime categorization for these events by combining a technology and a human component. If the cyber-attack contained mainly technological components, it was denominated type 1, and type 2 if the components were mainly human in nature. They further characterized type 1 events as singular or discrete from the perspective of the victim, facilitated by the use of crime-ware software and that the introduction of this software may not necessarily be facilitated by vulnerabilities. On the other hand, they characterized type 2 events as facilitated by processes that do not fit

under crime-ware (e.g., Instant Messaging, FTP file transfer), and as having in general repeated contacts or events from the perspective of the user.

Simmons et al., (2014) developed a cyber-attack taxonomy derived from computer program security flaws, which classifies threats according to potential defences, and thus facilitating the proposal of strategies to manage these risks. Through the identification of the ways in which attacks could take place, this group proposes a series of "vectors" which form the evaluation framework AVOIDIT (Attack Vector, Operational Impact, Defence, Information Impact, and Target). This framework uses a tree structure to categorize and enumerate the ways in which an attack might occur.

On the other hand, an inductive approach has been followed by organizations who monitor cyber-attack events to industrial organizations. These studies are normally presented as non-peer-reviewed articles or reports. This approach is inductive since it starts form the observable experience of cyber-attacks to industry, to subsequently propose a categorization or taxonomy that might be more generalizable. The incentives for private organizations to generate these reports is to evidence themselves as subject-matter-experts when offering cyber-security consulting services to industrial companies. Additionally, several multinational organizations have started regular updates on cyber security with information from its members, such as the Organization of American States (OAS, 2013), or the World Economic Forum (WEF, 2008).

Verizon (Verizon, 2014) has developed Data Breach Investigation Reports (DBIR), published yearly, and which gathers information about information breaches from 50 contributing organizations and spanning 95 countries around the world. This report identified 9 main types of breaches, i.e., cyber- espionage, DOS Attacks (denial of service), crime ware, web app attacks, insider misuse, miscellaneous errors, physical theft and loss, and payment card skimmers. These attack patterns described 92% of the 100.000 incident database taken into consideration by this study.

The OAS is issuing a yearly report that shows a 12-40% increase in reported cyber-attack incidents yet indicates in their latest report, "most states do not differentiate between the types or severity of cyber incidents they reported", and that "divergent views show that more specific data is needed to accurately diagnose the threat" (OAS, 2013).

The World Economic Forum (WEF, 2015) identified cyber risks as a high-impact technological risk and ranked it as above average both in likelihood and impact with respect to other types of risks. The WEF also makes a distinction between state-sponsored, state-affiliated, criminal, and terrorist cyber-attack types.

Supply chain resilience frameworks

The earliest reference to supply chain resilience frameworks found in our literature research corresponds to the frameworks proposed by Christopher & Peck at Cranfield University (Christopher el at, 2004), and the framework proposed by Sheffi & Rice at MIT (Sheffi et al., 2005). These approaches were largely complementary, both descriptive in nature and with some points in common such as the requirement for a risk culture in the organization as well as the explicit indication of a necessary trade-off between redundancy and efficiency at the time or developing organizational resiliency. However, while Christopher talks about capabilities required for resilience building and critical path identification, Sheffi concentrates on the analysis and mapping of vulnerabilities, and describes the dynamic behaviour of the performance of a supply chain through a disruption, proposing the concept of "disruption profile", with the qualitative identification of eight main phases within this disruption profile. Additionally,

Christopher emphasizes on "agility" for the deployment of existing resources (resulting from velocity and visibility within the organization) as a requirement for resilience, while Sheffi talks about "flexibility" and the transitory, alternate use of existing resources.

Subsequent models build on these initial frameworks, and are characterized by approximations to the empirical quantification of resilience through case studies. Blackhurst (Blackhurst et al., 2011) and her team in 2011, identified thirteen resilience enhancers and seven resilience reducers in the organization. On the other hand, Pettit & Fiskel (Pettit et al., 2010) from Ohio State University, proposed a SCRAM framework (supply chain resiliency assessment and management) in 2010. Through case studies, Pettit identifies seven "vulnerability factors" and fourteen "capability factors". Additionally, Pettit identifies an existing trade-off between developing too many unused capabilities through excessive investment, which would erode profits, versus developing too many vulnerability factors through insufficient investment, which would also erode profits through insufficient response to disruptions.

Work by Linkov (Linkov et al, 2013) at Arizona State University together with the US Army in 2013, proposes the concept of cyclic disruption event management through which an organization will need to prepare, absorb, recover from and adapt to disruptions, point at which a new cycle begins.

A summary of the chronology and relationship between these frameworks is presented in Figure 1:

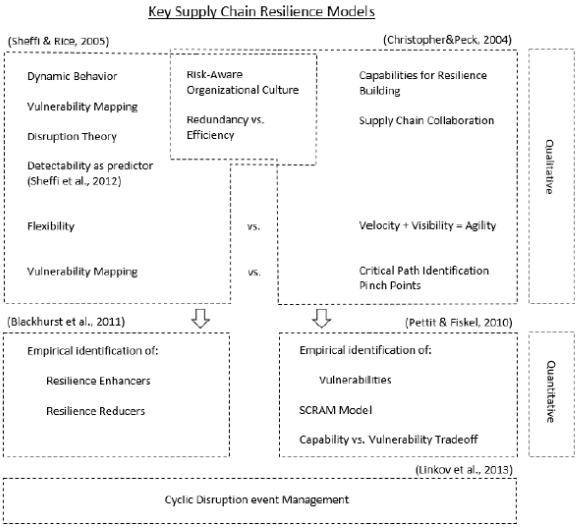

Figure 1 Key supply chain resilience models

In a recent 2014 article, Simchi-Levi at MIT described a technique for assessing the effect of disruptions on a supply network through the use of Time to Response - TTR, Performance Impact scores – PI, and a Risk Exposure Index – REI (Simchi-Levi et al., 2014). This method simulates the disruption response of a system by removing one node in the supply system at a time during the TTR, and optimizing system response, thus obtaining a PI for each node. The node with the largest PI is assigned a REI of 1,0, and the other nodes are assigned a REI relative to this Larges Rei value. These authors claim this method to better guide investment in areas with the greatest impact, is based on numerical optimization, and as a simulation it allows for experimentation with different TTR values.

Literature has documented the limitations of current risk assessment methods (Khan et al., 2007). These introduce assessment team biases, have a strong influence of past subjective experiences, are largely linear and static analyses, and deliver little information towards managing exposure to new or extreme events. Additionally, the assessments results can show a misalignment with management processes, hindering or delaying the implementation of assessment recommendations (Osha, 2008).

If the risk assessment of potential events is based on the experience of the team making the assessment, it is expected that the results will always run behind the new emergent modes of attack, characteristic of the cyber threats.

Discussion: Gap identification and tool proposals

Our literature research appears to show some initial proposals for a research agenda in the area of supply chain resilience in general (Khan & Zsidisin, 2011), and cyber resilience in particular (Khan & Sepulveda, 2015). We propose that this, as yet, limited literature on the topic is founded both in 1) a lack of evidence of a systemic perspective of the problem landscape to define a coherent problem space and thus guide research efforts, and 2) the lack of proposed complementary tools to established supply chain risk assessment methods, which may introduce ways of quantifying the dynamic response of a supply chain to disruptions starting from a familiar paradigm to practitioners.

As potential contributions to bridging the gap, this paper will argue for the use of a systemic analysis of the problem landscape description, as well as for the use of detectability for quantifying the dynamic response of systems by adding this parameter to existing FMCA (Failure mode and Criticality Analysis) processes.

Tool type 1: Systemic outlook of the problem landscape

Our literature research did not find any systemic analysis of the cyber risk issue, which might illustrate, even in qualitative terms, the relationships between the different agents in the problem, and which might account for both short and long-term impacts. System dynamics tools such as causal loop diagrams (CLD) and stock and flow diagrams (SFD) and can be used to map out and quantify the known relationships that exist between actors within a complex system (Sterman, 2000), and in order to explore and understand the evolution of these relationships and behavioural feedbacks over time. Such a diagram/model will be by definition an approximation to reality, and has to have a correct balance between aggregation and atomization of variables for the problem we are trying to describe.

It is relevant to keep in mind the interaction between the static configuration of a system and its dynamic behaviour. This is shown in Figure 2.

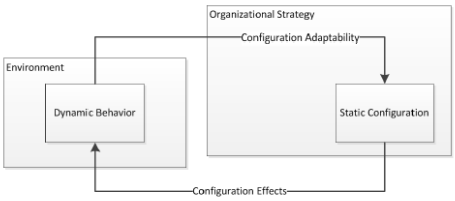

Figure 2 Relation between supply chain dynamic behaviour and static configuration

Figure 2 shows a feedback loop between an organization's supply chain static configuration and the dynamic behaviour of this supply chain when subject to its environment. This dynamic behaviour then feeds back into, and adjusts the static configuration according to the available adaptability skills in the supply chain, in an ongoing, circular process.

Since the resilience of an organization in general, and cyber-resilience in particular is not an event, but a series of connected events which develop in time as a result of an underlying system structure (i.e., behaviour), traditional methods of risk analysis fall short of describing these behaviours correctly, and we argue are ill-equipped to manage these types of problems. This is tantamount to explaining why breaks are necessary or how they should be used in a car, by analysing a series of photos of the car in movement; no amount of photos will correctly convey the effects of the car mass or velocity, for example, in how the breaks should be applied.

A first approximation to a causal loop diagram of the problem of cyber-attacks to supply chains is shown in Figure 3. This diagram shows three main social spaces where this problem develops. The company space reflects the dynamics within an industrial organization that promote or hinder investment in cyber-capabilities, how this investment relates to the vulnerabilities and resulting number of cyber-attacks, and finally the effect this has on customer satisfaction. The hacker space shows the internal process of hacker prestige and hacker legal prosecution which respectively promote and hinder the development of cyber-attack modes and the number of cyber-attacks. It is important to note that these two spaces in this model share at least the number of attacks and the technology available. A third space, the public space is present as it creates the social tension to promote prosecution of hackers due to the lower level of customer satisfaction which results from the hacker attacks.

A next step after a systemic understanding of the problem landscape, but to which no tools have yet been proposed, is to investigate and analyse the dynamics of the system. To this end, an SFD is necessary, which not only quantifies the relationships between actors that were identified in the CLD, but also integrates dynamic effects such as sources of systemic inertia, important delays in the relationships, as well as the identification of policy levers.

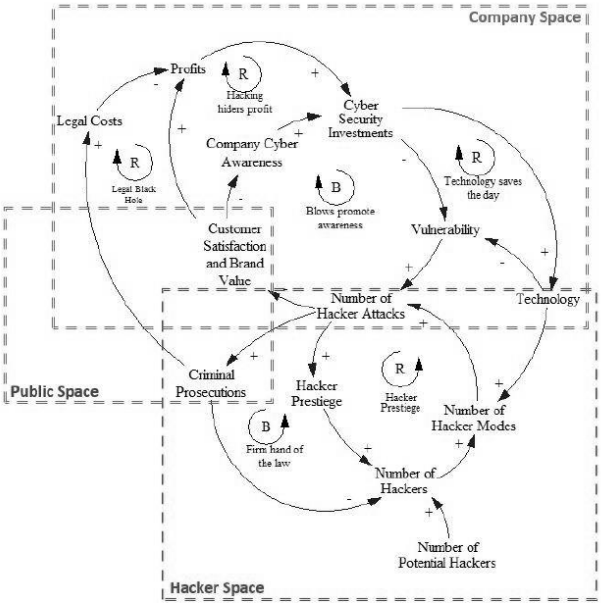

Figure 3 Systemic Analysis if the Problem Landscape

Tool type 2: Bridging the gap- Dynamic response through detectability

Dynamic behaviour is not an easy subject to convey to practitioners. Therefore a second type of tool proposed in this work relates to tools, which might help manage these effects in time, through complements to tools which have practitioner use and acceptance.

Detectability as a risk assessment factor in supply chain risk management had been proposed in the past (Sheffi et al., 2012; Lee, 2007) but has eluded widespread application for risk assessment processes, as detectability is considered by some a damage-containment (event mitigating) parameter, more than a risk mitigation factor (Youssef et al., 2010). Others argue the counter-intuitive nature of the event detectability when used in conjunction with probability and severity: while the higher probability or severity associated with a supply chain risk relate to a disruption event that is more relevant, a higher detectability, corresponds to an event that is in fact less relevant. Therefore, measures of "un-detectability" have rather been suggested.

We argue here that it is a convenient way to reflect the degree of perceived resilience in the organization, and therefore of its dynamic response to disruptions. Based in the disruption model presented by Sheffi & Rice (Sheffi et al., 2004), consider the evolution of a supply chain process KPI through a disruptive event, as illustrated in Figure 4:

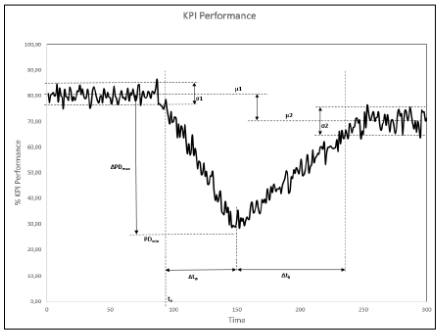

Figure 4 Quantitative description of a disruption event curve

This generic KPI, before the disruptive event had an average value of μ_1 and a standard deviation of σ_1. At time t_0 this supply chain starts to experience a decrease in this KPI beyond the normal levels. This reduction in performance continues to a point when the organization reacts and the performance reverts its downward trend at time $t_0+\Delta t_w$, reaching a new level of stable operation at time $t_0+\Delta t_w+ \Delta t_b$, with a new mean value for this KPI of μ_2 and a standard deviation of σ_2. At this point we make a proposition for the characteristic of this process development:

Proposition 1: The unwanted organizational effects of a disruptive event will have a direct relationship with the total duration of the disruption (Δt_w and Δt_b in Figure 4

Proposition 2: The unwanted organizational effects of a disruptive event will have a direct relationship with the decrease in the performance of the supply chain through the duration of the disruption (ΔPD_{max} in Figure 4)

Now, consider two equivalent processes with different detectability. The effect of this difference when subjected to a disruptive event can be illustrated in Figure 5.

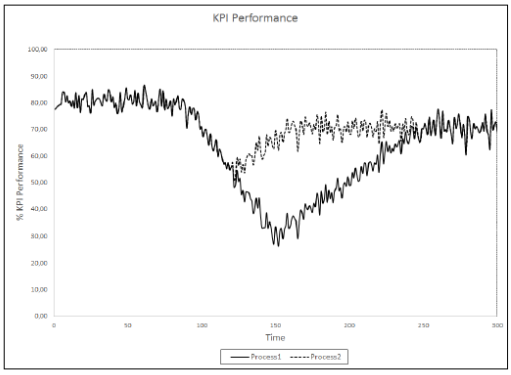

Figure 5 Process comparison

Process 2 as illustrated, has a better detectability (i.e., starts earlier with its KPI performance recovery) and is likely to have a smaller organizational adverse effect than Process 1. Hence, Process 2 could be identified as more resilient than Process 1. This earlier reaction in Process 1 can occur due to any combination of a series of organizational capabilities, among them, "awareness" to identify unusual operating conditions, which trigger disruption mitigation actions, and /or "flexibility", to quickly generate the organizational adaptations for disruption mitigation. These capabilities relate to the "agility" factor for supply chain resilience identified by Christopher (Christopher et al., 2003). Additionally, the way these capabilities interact during a disruption event, and how these capabilities and system structure relate to cyber-attack effects should be analysed through a systemic model.

Such a tool would be especially well suited to supply chains where KPI performance measurement is already taking place frequently or online. The quantity and speed with which cyber-attacks affect supply chains, makes these type of tools especially well suited to these types of risks. The methods for such an implementation stand out as relevant research opportunities derived from this work.

Conclusions

The relevant adverse effects, as well as the increasing number of cyber-attacks on supply chains, together with the limited research that has been undertaken to describe and manage this phenomenon, makes this a very significant area of research.

Additionally, any research that is conducted on cyber risk in the supply chain will necessarily need close interaction with practitioners, in order to keep up with the speed of development of these types of threats, towards shorter cycles of tool development, tool proposal and tool validation. Furthermore, a comprehensive research framework which has identified all relevant actors and stakeholders in the supply chain and problem landscape and has made informed decisions on the priority of cyber resilience development for each supply chain area and system participant, should be developed.

This paper lays out proposals for bridging some relevant gaps, which serve as stepping stones towards tools and methods which might be both accepted and applicable by practitioners, as well as coherent with a systemic understanding of the complex problem of cyber risks and security in the global supply chain.

References

Blackhurst, J., Dunn, K., Craighead, C. (2011), "An empirically derived framework of global supply resiliency", *Journal of Business Logistics*, Vol. 32, No. 4, pp. 374-391.

Christopher, M., Peck, H. (2003), "Supply chain resilience, final report on behalf of the department of transport", *University of Cranfield*.

Christopher, M. (2011), "Logistics and Supply Chain Management", *Financial Times Series*, London, p.213.

Dederick, J., Sean, X., Zhu, K. (2008), "How does information technology shape supply chain structure? Evidence on the number of suppliers", *Journal of Management Information Systems*, Vol. 25, No. 2, pp. 41-72.

Doyle, J.,Ford, D. (1998), "Mental models concepts for system dynamics", *System dynamics review*, Vol. 14, No. 1, pp. 3-29.

Gordon, S., Ford, R. (2006), "On the definition and classification of cybercrime", *Journal of Computational Virology*, Vol.2, pp. 13-20.

Khan, O., Burnes, B. (2007), "Risk and supply chain management: creating a research agenda", *The International Journal of Logistics Management*, Vol. 18, No. 2, pp. 197-216.

Khan, O. Zsidisin, G. (2011), "Handbook for Supply Chain Risk Management: Case Studies, Effective Practices and Emerging Trends", *J. Ross Publishing*

Khan, O., Sepulveda, D.A. (2015), "Supply Chain cyber resilience: crating an agenda for future research", *Technology and Information Management Review*, Vol. 5, No. 4

Lee, W. (2007), "Risk Assessment modelling in aviation safety management", *Journal of Air Transport Management*, Vol. 12, No. 5, pp. 267-273.

Linkov, I. (2013), "Measurable resilience for actionable policy", *Environmental science & technology*, Vol. 47, No. 18, pp. 10108-10110.

OAS. (2013), "Latin American and Caribbean cybersecurity trends and government responses", *http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-latin-american-and-caribbean-cybersecurity-trends-and-government-responses.pdf*, access 30 April 2015.

Pettit, F., Croxton, K. (2010), "Ensuring supply chain resilience: development of a conceptual framework", *Journal of Business Logistics*, Vol. 31, No. 1, pp. 1-21.

Simchi-Levi, D., Schmidt, W., Wei, Y. (2014), "From superstorms to factory fires: managing unpredictable supply-chain disruptions", *Harvard Business Review*, Vol. 92, No. 1-2, pp. 96.

Sheffi, Y. (2005), "The Resilient Enterprise", *MIT Press Books*, pp. 14.

Sheffi, Y., Vakil, B., Griffin, T. (2012), "Risk and Disruptions: New software tools", *http://sheffi.mit.edu/sites/default/files/Risk_and_Disruptions_V9.pdf*, access 30 April 2015.

Simmons, C. (2014), "AVOIDIT: A cyber-attack taxonomy", *9th annual symposium on information assurance* (Asia '14).

Sterman, J. (2000), "Business Dynamics", *Irwin/McGraw-Hill*, Boston, pp. 1-39.

Tranfield, D., Denyer, D., Smart, P. (2003), "Towards a methodology for developing evidence-informed management knowledge by means of systematic review", *British Journal of Management*, Vol. 14, No. 3, pp. 207-222.

Verizon. (2014), "2014 Data Breach Investigations Report", *http://www.verizonenterprise.com/DBIR/*, access: 30 April 2015.

WEF. (2008), "Global risks landscape 2015", *http://www3.weforum.org/docs/WEF_Global_Risks_2015_Report15.pdf*, access: 30 April 2015.

Youssef, N., Hyman, W. (2010), "Risk analysis: Beyond probability and severity", *Medical Device and Diagnostic Industry*, Vol. 32, No. 8.

11.6.4 Paper 4

Control structures in supply chains as a way to manage unpredictable cyber-risks

Daniel A. Sepulveda Estay (dasep@dtu.dk)
Management Engineering, Technical University of Denmark

Omera Khan
Product Operations Management, Aalborg University

Summary Abstract
Supply chain growth, and their dependence on Information Technology (IT), is making cyber risks an increasingly unmanageable threat through traditional risk assessment methods. Systemic analysis methods have been identified as alternatives to traditional methods. This paper analyzes the application of a systemic risk analysis methodology to understand cyber risks in the supply chain. A generic supply chain is analyzed, and information flows, dynamic structures and the influence of cyber-attack on these are identified. This paper argues that a systemic approach is more efficient in detecting vulnerabilities, enabling an evolving disruption response process and culture in the supply chain.

Keywords: Cyber-risks, Supply Chain Management, Resilience

Introduction
In recent years, supply chains have increasingly grown in complexity, coupled by their dependence on Information Technology (IT), in becoming what has been defined as cyber-physical systems, or the embedding of IT in applications in the real world (Gollmann et al., 2016). Although this complexity has allowed a faster operation and frontier-less communication, it has also exposed supply chains to new vulnerabilities (Manuj et al., 2008) because of the increased number of nodes and connections present in the cyber supply chain (Dederick et al., 2008). Disruptions resulting from these vulnerabilities have been placed at US 300 billion in losses and, not surprisingly, cyber-attacks have been identified as one of the most important risks in the supply chain (WEF, 2013).

Cyber risks in the supply chain, i.e., those risks associated with the use of IT, differ substantially from other supply chain risks that may be present. Some of these differences are summarized in Table 1, including aspects such as physical location, complexity limitation, and anonymity.

Table 1: Cyber versus Physical Risks in the Supply Chain

Physical Supply Chain (Flow of goods)	**Cyber Supply Chain (Flow of Information)**
Physical location is relevant	Physical location is irrelevant
Anonymity is uncommon	Anonymity is common
Limited complexity	Unlimited complexity
Buffers are useful	Buffers are risky
Mainly components risk	Mainly interaction risks

Companies have been managing risks in their supply chains through causal chain analysis techniques, primarily with a focus on its physical dimension, such as Failure Tree Analysis (FTA), Failure modes and criticality analysis (FMECA), or through probabilistic methods. For systems with limited complexity and mainly focused on component performance, these techniques have been useful.

However, two main issues stand out. First, with the increase in supply chain complexity, these techniques are increasingly onerous to implement and maintain. In order to consider all potential modes of failure, important resources are required to create these traditional risk analyses or to maintain them as existing risks change or new ones appear. Second, Supply chain IT development has allowed both a decrease in the individual supply chain component failure, as well as an increase in the number of interaction failures in the supply chain.

This means that a supply chain can fail even if all its components worked as expected, as the risk is materialized in the interaction between these components, situation that would be invisible to traditional methods, centered on component reliability and direct contributing factors to the specific risk. This is rendering traditional risk methods increasingly inadequate for the complex systems in which they need to be used. The following table summarizes some of the reasons why traditional approaches are insufficient for the modern supply chain.

Table 2: Traditional way versus their insufficiency

Traditional way	**Reason for insufficiency**
Focus is on structure-to-risk	Nothing is said about reaction-to-risk
Focus is on components	Nothing is said about the interaction between these components
Prepares organization for specific risks	Organization needs to react to any risk
Human effects are centered around operator error	Human effects can lead to risk even if no operator error is made
Assumes a constant structure	Structure is changing continuously

A first aspect for inquiry is exposed at this point, regarding other tools that might exist to deal with these insufficiencies. This paper proposes additional approaches that may complement traditional analyses, and which might bridge the insufficiencies listed above addressing not only preparation for cyber-risks, but also reaction to cyber risks, i.e., cyber-resilience.

Additional to causal chain and probabilistic analyses, a third approach has been proposed in literature to understand risk, namely systemic risk analysis. This approach seeks to change the problem management from one of individual component reliability (i.e., each part of the supply chain functions as it is supposed to do), to a control problem of the complete relevant

supply system. Techniques such as the Systems Theoretic Accident Model & Processes (STAMP) have been used areas such as product development, and manufacturing operations, and its advantages and outcomes have been well documented for these cases (Altabbakh et al., 2014). However, systemic methods of analysis have been used to analyze supply chains only in a limited way. A second aspect of inquiry is thus the way in which systemic analyses of cyber risks, allow us to better understand and manage these risks in supply chains.

Cyber resilience in supply chains

According to Christopher and Peck, supply chain resilience is the ability of a supply chain to return to its original state or move to a new, more desirable state after being disturbed (Christopher et al., 2004). Supply chain resilience has thus evolved as an additional concept to supply chain risk. While risk management entails the examination of all possible outcomes of a process, weighing the potential returns against the potential risks of investment, resilience management characterizes organizational reaction to low probability / high impact events and unforeseeable disruptions to create competitive advantage (Petit et al., 2010).

Literature has taken different perspectives to examine supply disruptions and resilience in supply chains, such as conceptual (Christopher et al., 2004), behavioral (Ellis et al, 2010), qualitative (Sheffi et al, 2005; Craighead et al, 2007), simulation/modelling (Wu et al., 2007; Nair et al., 2011), and network structure (Kim et al., 2015). Such a variety of approaches has enabled a number of different ways in which to understand the phenomenon, yet has also led to a degree of confusion about the level of analysis appropriate for different situations.

All the approaches to supply chain resilience are static except for Sheffi and Rice's proposal (Sheffi et al., 2005), which consisted of the application to supply chains of a disruption theory for production systems developed in Norway (Absbjornslett, 1999), proposing what was defined by them as the "disruption profile". This approach is identified as dynamic since the response of the supply chain changes over time, and is qualitatively described through eight distinct phases of evolution, i.e., preparation, disruptive event, first response, initial impact, time of full impact, preparation for recovery, recovery, and long-term impact (Sheffi et al., 2005). However, none of the definitions of resilience found in our literature review has considered system control as part of their definition.

The other approaches to supply chain resilience describe the supply chain at a specific point in time, and are thus static in nature, akin to taking a picture of the current state of the supply chain resilience. Moreover, many of the definitions present in literature, such as Tang (Tang, 2006) or Longo & Oren (Longo & Oren, 2008), limit their contribution only to proposing a definition for resilience, without the subsequent suggestion of any qualitative description, or quantitative measure of this supply chain resilience.

Starting from Sheffi & Rice's approach, Khan and her team have proposed that the length and depth of the disruption can be considered as a direct indicator of the resilience of a process, as can be seen in Figure 1. If a process has a longer disruption in its performance and/or a performance disruption is greater, then it can be said to have a lower/weaker resilience (Khan et al., 2015).

Although these measures might make sense for simple systems, it is not clear if they will have similar effects to complex interconnected supply networks. For example, Kim and his team have already suggested that redundancy might hinder resilience for some supply network configurations (Kim et al., 2014). It has also been mentioned that redundancy can be effective systems consisting of purely electromechanical components. However, when

there is software involved as well as the interaction of human operators, redundancy can sometimes contribute to accidents through, e.g., design complexity (Leveson, 2011).

Systemic risk analysis methods.

The use of feedback loops for a systemic understanding of risk in industrial systems including the human component is not new. In 1998, the analysis of industries with high levels of hazard (Carroll, 1998), suggested that traditional solutions, although well-intentioned, fail to help through their unintended side-effects, as illustrated in the Figure 1.

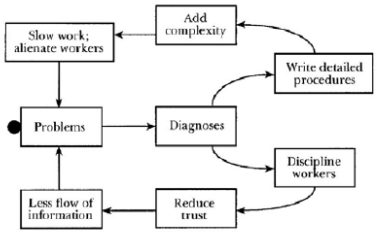

Figure 1: Common mitigation measures and their side effects (Carroll 1998)

Kang and his team have used a systems approach to identify Limiting Conditions for Operation (LCOs in operations, extensible to supply chains (Kang et al., 2005). Their approach acknowledges three important aspects: 1) a system dynamics approach ensures a causal relationship in the establishment of the feedback loop structure, 2) the approach is useful for understanding the behavior of a complex system over time, and 3) a systemic approach is useful in conceptualizing a thorough understanding of human interactions within complex systems.

More recently, Gahdge et al., (2013) proposed a systemic approach based on the three pillars of risk identification, risk assessment and risk mitigation. Through the generation of a system dynamics model containing different attributes and parameters, risks can be simulated and sensitivity analyses can be obtained on the relevance of each parameter. However, although the results and simulation clearly point out to a system dynamics model, it is unclear what feedback loops, delays and sources of inertia, i.e., stocks (Sterman, 2000) were considered.

Garbolino et al. (2016) and his team used system dynamics modeling and risk analysis to propose a dynamic risk analysis method that includes both approaches. They acknowledge that this modelling approach focuses on the strengthening of constraints, and it allows a dynamic process where industrial systems continually adapt to external and internal changes to achieve their goals. They propose a ten-step approach that results in scenario analysis through a model. It is however restricted to a single plant and its internal process, thereby lacking the integration with other supply partners.

Our research process did not find documented literature on the application of systemic risk analysis methods to supply chains.

Research Hypothesis

This paper considers three main hypotheses that direct the choice and application of different frameworks for understanding cyber-risks in the supply chain.

First, supply chains have structures that determine how they react over time to disruptions such as cyber-attacks. According to the System Dynamics approach, an observed behavior in a supply system is the result of an underlying structure (Forrester, 1961; Sterman, 2000). In a supply chain, these cause either the flow of physical goods (e.g., raw materials, physical products, and physical services) or a flow of information (e.g., Purchase Orders, Money, Coordination emails, digital products or services).

Second, physical flow of goods is controlled by the information flow around that process. The physical flow follows the instructions laid down by the information flow in the supply chain. Closed loop control structures involve feedback loops (Doyle et al., 1992), and it is expected the same thing will happen for the case of supply chains.

Third, cyber-attacks to a supply chain will necessarily affect its information flows, and involve one or more feedback loops, which are then later reflected as an operational disruption.

Methodology

The process that was followed for the analysis of a supply chain through a systemic risk analysis follows the STAMP model (Systems-theoretic Accident Model and Processes) as proposed by Leveson (2011). This paper does not explain the methodology, rather focuses on the results and consequences of its application to cyber risks in the supply chain.

This is a model based on systems theory rather than traditional analytic reduction and reliability theory. A safe operation is seen as an emergent property resulting from the interactions of the components with each other and the environment. The problem of avoiding "accidents" (unplanned loss events) thus becomes a dynamic control problem. Figure 3 shows a control system representation of a controlled process. Only an extract of the analysis is shown.

Results

Control systems representation

Let us consider a simple supply chain as a single-level transaction between a buyer and a seller, for the ownership of a product.

This single-level supply chain already involves at least three members, i.e., buyer, seller, transporter, also known as "agents" (Swaminathan et al., 1998). Through such a process, a buyer will inform a seller that it wants to buy an item from them. The seller agrees, and contacts a transportation agent to move the product from the seller to the buyer. The representation of such a supply chain is a reflection of the information gathered on how such a supply chain is working, and is by definition, incomplete (Sterman, 2002). The information flow present in this simple supply chain is not linear and it requires many flows of information, between the different agents involved, as represented in Table 3.

Table 3 Information Flows in generic 1-level supply chain

Information Flow Number	Description	Emiting agent	Receiving Agent	Required Predecesor
IFL1	Purchase Order (P.O.)	Buyer	Seller	-
IFL2	P.O. Confirmation	Seller	Buyer	IFL1
IFL3	Service Order (S.O.)	Seller	Transporter	IFL2
IFL4	S.O. Confirmation	Transporter	Seller	IFL3
IFL5	Pickup Coordination	Transporter	Seller	IFL4
IFL6	Delivery Coordination	Transporter	Buyer	IFL4
IFL7	Transport Documentation	Transporter	Seller	IFL4
IFL8	Transport Documentation	Seller	Buyer	IFL2
IFL9	S.O. Payment	Seller	Transporter	IFL7
IFL10	S.O. Payment Confirmation	Transporter	Seller	IFL9
IFL11	P.O. Payment	Buyer	Seller	IFL8
IFL12	P.O. Payment Confirmation	Seller	Buyer	IFL11

As it can be seen, these information flows are not isolated and in themselves may require a specific flow predecessor to take place. For example, in order that IFL-2 can happen (Purchase Order Confirmation) from the seller to the buyer, a previous purchase order information flow must have been emitted by the buyer to the seller, i.e., IFL-1. These create feedback loops, which can be identified in the following control loop diagram in Figure 2. The loops involved are mentioned in Table 4.

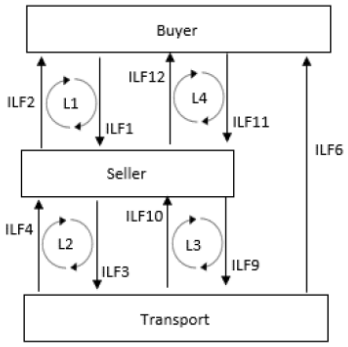

Figure 2: Basic information supply chain (partial representation of flows).

Table 4 Information Feedback Loops for a single-level supply chain

Control Loop	Description	Information Flows (IFL) involved
L1	Purchase Order Loop	IFl1 - IFL2
L2	Service Order Loop	IFL3 - IFL4
L3	S.O. Payment Loop	IFL9 - IFL10
L4	P.O. Payment Loop	IFL11-IFL12

Table 5: Analysis if unsafe control actions from a cyber-attack (Extract)

UCA	Desc.	Type 1	Type 2	Type 3	Type 4
UCA #1	Send Service Order to Transport Agent	Seller does not send service order to transport agent, when there has been a confirmed purchase order Transport agent does not receive the service order sent by the seller.	Seller sends service order confirmation to buyer with the wrong product specification. Buyer receives the purchase order confirmation with the wrong product specification. Seller sends purchase order confirmation considering inaccurate stock information.	Seller sends service order to transport agent too late to arrange a timely pickup/delivery	not applicable (Service Order is either sent or not)
UCA #2	Send Purchase Order confirmation to buyer	Seller does not send the purchase order confirmation to buyer when there has been a purchase order received. Buyer does not receive the purchase order confirmation sent by the seller	Seller sends purchase order confirmation to buyer with the wrong product specification. Buyer receives the purchase order confirmation with the wrong product specification. Seller sends purchase order confirmation considering inaccurate stock information.	Seller sends the purchase order confirmation to buyer before identifying existing stock.	Not applicable (Purchase Order Confirmation is either sent or not)
UCA #3	Send service order confirmation	Transport Agent does not send the service order confirmation to the seller when there has been a service order received The seller does not receive a service order confirmation, when it has issued a service order to the transport agent.	Transport agent sends service order confirmation with wrong specifications which are then later confirmed with buyer	Transport agent send service order confirmation to seller too late to make timely pickup arrangements	Not applicable (Service Order Confirmation is either sent or not)

7

Hazard Analysis

For a generic, single-tier supply chain, the accidents and unacceptable losses in the case of cyber-attacks to supply chains have to be defined. This is highly dependent on the specific supply chain, and in the case of a generic supply chain example, a few examples are mentioned in the following table.

Table 6: Unacceptable accidents in the supply chain (extract)

Accidents	Description
A1	No product is delivered to customer due to cyber-attack
A2	Wrong product is delivered to customer due to a cyber attack

The system as defined has different control actions, for the hazards that can be identified. These can have four types of dangers. (Leveson, 2011). Type 1: The control action is present, thus causing an unsafe conditions; Type 2: The control action is absent, thus causing an unsafe condition; Type 3: The control action was applied to early or too late, thus causing an unsafe condition, and Type 4: The control action was applied to little or too much, thus causing an unsafe condition.

An extract of the type of analysis that can be achieved for a generic supply chain, starting from each Unsafe Control Action (UCA) is shown in the following Table 5.

Discussion

This paper proposes a detailed and concise way of representing the flow of information/communication for a simplified, generic supply chain. This representation was based on the identification of the relevant supply system, the agents interacting in the supply system, the communication paths, and the resulting feedback loops. Control structures were identified in the supply chain as a result, based on the communication flows present.

The example presented in this paper is not intended to be an exhaustive analysis of a supply, but rather sought to show the application of a systemic risk analysis technique to the case of cyber risks in the supply chain.

This is a novel approach and does not contradict other static frameworks for resilience (Christopher et al., 2003), and builds from the original "disruption curve" by Sheffi & Rice (Sheffi et al., 2005), expanding the theory by proposing mechanisms through which this behavior over time is achieved in a supply chain after a cyber-attack (cyber-resilience).

The proposal of a control structure for supply chains is consistent with other equivalent structures that have been studied in different fields of knowledge.

The explicit representation of information flows through an information flow map, has been shown to enhance team productivity and effectiveness. From this simplified system representation, four relevant insights can be derived. First, some information flows may not be present. This should trigger analyses on the need to include or exclude them. Second, some information flows will not be part of a loop. This might be the reflection of a fixed procedure in place. If there is control required on these flows, then a loop has to be completed. Third, there may be redundant information flows. This should be looked at carefully to identify the situations where this dual information flow might lead to a risky situation. Fourth, some of these information flows may not be electronic, thus not subject to cyber hacking, yet also not subject to electronic recording or with the possibility of automated control.

Some recommendations can be derived from this work.

- Understand the information flows in your supply chain.
- Control structures involving information flows in supply chains span over different areas of the company, requiring the interaction of different departments during a cyber-attack.
- The focus of the management of cyber-risks should also include the management of the systemic structure (requirements and constraints) as well as interactions, both high leverage options, and not merely the static structure and correcting of behavior.
- The process of hazard and requirements identification is an ongoing, cumulative process that is adjusted by new hazards as these are identified and integrated into the analysis.

Some of the insufficiencies mentioned in Table 2 are initially addressed through the use of this methodology for the case of supply chains. The focus is on reaction-to risk, it describes explicitly the interactions between components and can integrate redundancy as source of cyber-risks.

Conclusions and future work

This paper develops a first approach to represent the response of supply chains to disruptions caused by cyber-attacks, and proposes a structured methodology for the identification of vulnerabilities and the constraints that condition this supply chain response.

The analysis results in some general recommendations for constraints and requirements. The main areas where future work is recommended include the application to ex-post examples, the quantification of the effects of different factors and their relationship to the resulting cyber-resilience of the supply chain, and performance testing under different scenarios for varying requirements and constraints.

This approach to understanding cyber risks as a dynamic control problem needs to be implemented ex-ante for other cases, to identify constraints. There is also a potential for a network representation of the information flows, and of researching potential applications of network theory for understanding the existing relationships in supply chains.

References

Altabbakh, H., Alkazimi, M. A., Murray. S., Grantham, K., 2014. STAMP – Holistic system safety approach or just another risk model?, Journal of loss prevention in the process industries, 32, pp. 109-119.

Asbjornslett, B. E., 1999. Assess the vulnerability of your production system. Production Planning & Control, 10(3), pp. 219–229.

Carroll, J.S., 1998. Organizational learning activities in high-hazard industries: the logics underlying self-analysis. Journal of Management studies, 35(6), pp.699-717.

Christopher, M., Peck, H., 2004. Building the resilient supply chain. International journal of Logistics Management. 15(2), pp. 1-14.

Collmann, D., Krotofil, M., 2016. Cyber-physical systems security, Lecture notes in Computer Science, Vol 9100, pp.195-204, Springer, DOI: 10.1007/978-3-662-49301-4_14.

Craighead, C. W., Blackhurst, J., Rungtusanathan, M. J., Handfield, R. B., 2007. The severity of supply chain disruptions: design characteristics and mitigation capabilities. Decision Sciences 38(1), pp. 131-156.

Dederick, J., Xin Xu, S., Xiaoguo, K. Z., 2008. How does information technology shape supply-chain structure? Evidence on the number of suppliers. Journal of Management Information Systems, 25(2), 41-72.

De Oliveira, E., Werther Jr., W.B., 2013. Resilience: continuous renewal of competitive advantages. Business Horizons 56(3), pp. 333-342.

Doyle, J., Francis, B., Tannenbaum, A., 1992. Feedback Control Theory, New York, Dover Publications

Ellis, S. C., Henry R. M., Shockley, J., 2010. Buyer perceptions of supply chain disruption risk: a behavioral view and empirical assessment. Journal of Operations Management, 28(1), pp. 34-46.

Forrester, J., 1961. Industrial Dynamics, System Dynamics Series, Pegasus Communications.
Garbolino, E., Chery, J. P., Guarnieri, F., 2016. A simplified approach to risk assessment based on system dynamics: an industrial case study, Risk Analysis (2016).
Ghadge, A., Dani, S., 2013. A systems approach for modelling supply chain risks, Supply Chain Management: An international Journal, 18(5), pp. 523-538.
Ishimatsu, T., Leveson, N.G., Thomas, J., Katahira, M., Miyamoto, Y. and Nakao, H., 2010. Modeling and hazard analysis using STPA.
Johnson, N., Elliott, D. and Drake, P., 2013. Exploring the role of social capital in facilitating supply chain resilience. Supply Chain Management: An International Journal, 18(3), pp.324-336.
Jüttner, U. and Maklan, S., 2011. Supply chain resilience in the global financial crisis: an empirical study. Supply Chain Management: An International Journal, 16(4), pp.246-259.
Kang, K. M., Jae, M, 2005. A quantitative assessment of LCOs for operations using system dynamics, Reliability Engineering and System Safety, 87, pp.211-222.
Kim, Y., Chen, Y.S., Linderman, K., 2015. Supply network disruption and resilience: a network structural perspective. Journal of operations management, 33(2015), pp. 43-59.
Leveson, N., 2011. Engineering a safer world: Systems thinking applied to safety. Mit Press.
Longo, F. and Oren, T., 2008, September. Supply chain vulnerability and resilience: a state of the art overview. In Proceedings of European Modeling & Simulation Symposium (pp. 17-19).
Manuj, I., Mentzer, J. 2008. Global supply chain management strategies, International Journal of Physical Distribution and Logistics Management, 38(3), pp. 192-223.
Nair, A., Vidal, J. M., 2011. Supply network topology and robustness against disruptions – an investigation using multi-agent model. International Journal of Production Research, 49(5), pp. 1391-1404.
Petit, T. J., Fiskel, J., Croxton, K. L., 2010. Ensuring supply chain resilience: development of a conceptual framework. Journal of business logistics. 31(1), pp. 1-21.
Ponomarov, S.Y. and Holcomb, M.C., 2009. Understanding the concept of supply chain resilience. The International Journal of Logistics Management, 20(1), pp.124-143.
Salmon, P.M., Cornelissen, M. and Trotter, M.J., 2012. Systems-based accident analysis methods: A comparison of Accimap, HFACS, and STAMP, Safety science, 50(4), pp.1158-1170.
Scholten, K., Sharkey Scott, P. and Fynes, B., 2014. Mitigation processes–antecedents for building supply chain resilience. Supply Chain Management: An International Journal, 19(2), pp.211-228.
Sheffi, Y., Rice, J., 2005. A supply chain view of the resilient enterprise. MIT Sloan Management Review. 47(1), pp. 41-48.
Sheffi, Y., 2015. The power of resilience. The MIT Press, Cambridge, Massachusetts.
Sterman, J., 2000. Business Dynamics: Systems thinking and modeling for a complex world, Boston, Irwin/McGraw-Hill
Sterman, J.D., 2002. All models are wrong: reflections on becoming a systems scientist. System Dynamics Review, 18(4), pp.501-531.
Swaminathan, J.M., Smith, S.F. and Sadeh, N.M., 1998. Modeling supply chain dynamics: A multiagent approach*. Decision sciences, 29(3), pp.607-632.
Tang, C.S., 2006. Robust strategies for mitigating supply chain disruptions. International Journal of Logistics: Research and Applications, 9(1), pp.33-45.
WEF, 2013. Building resilience in supply chains. Industry agenda report. Accessed in 12 November 2015 at http://www3.weforum.org/docs/WEF_RRN_MO_BuildingResilienceSupplyChains_Report_2013.pdf.
Wu, T., Blackhurst, J., O'Grady, P., 2007. Methodology for supply chain disruption analysis. International Journal of Production Research, 45(7), pp. 1665-1682.
Zhao, K., Kumar, A., Harrison, T.P. and Yen, J., 2011. Analyzing the resilience of complex supply network topologies against random and targeted disruptions. Systems Journal, IEEE, 5(1), pp.28-39.

11.6.5 Paper 5

A system dynamics case study of resilient response to IP theft from a cyber-attack

D.A.Sepulveda[1], O.Q. Khan[2]
[1]Department of Management Engineering, Technical University of Denmark, Kongens Lyngby, Denmark
[2]Department of Business and Management, Aalborg University Copenhagen, Denmark
(dasep@dtu.dk)

Abstract - **Undesirable changes in supply chain physical operations derived from disruptions in the transmission or storage of digital information are reported daily despite the Information Technology (IT) protection available. Once a disruption materializes, the company losses will depend on the coherence and swiftness of the supply chain response (resilience). However, current resilience frameworks are qualitative, do not address evolution over time as a relevant aspect, and thus do not provide indications on how to design a resilient response. This paper contributes to closing this gap by developing a system dynamics model from an actual case of resilient response after a cyber-attack. Both case-specific and generic structures are extracted from the case data analysis, and a reaction mechanism is proposed that results in the observed behavior. The identification of these structures should eventually aid decision makers in the process of designing a resilient supply chain response.**

Keywords - Resilience, Cyber-risk, System Dynamics

I. INTRODUCTION

There has been an undisputed increase in the use of Information Technology (IT) in supply chains [1]. This trend is likely to continue as IT enables supply chains to respond to market pressures for efficient operation and customer collaboration during product and service delivery. However, the complex digital network that has resulted has created new sources of risk, mainly related to unintended system flaws that make user error more likely, and results in both internal and external risks [2]. Internal risks are derived from vulnerabilities in the connections between system components that result in risk of failure even if all parts of the supply chain work as expected, and external risks are derived from unauthorized agents exploiting these vulnerabilities for their own benefit.

Intellectual property (IP) is an example of a particular organizational asset which has increased its exposure to theft through the use of IT for its transfer, storage, and development coordination. IP is a central driver for innovation, business growth and competitiveness, potentially constituting as much as 80 percent of a single company's value [3]. Additionally, the Sarbanes Oxley regulation, enforced after the Enron and Worldcom scandals, has imposed accounting rules that result in a greater required detail in the reporting of IP valuation. This has transformed IP from being an internal strategic factor, to being a public financial dimension [4]. Literature informs that the most advanced economies are those with the greatest cyber-related IP losses, theft that accounted for as much of the US$ 200 billion cybercrime losses during 2013 [5].

Traditionally, IP took the form of people inside the organization, with direct knowledge and access to R&D resources, who misappropriated prototypes or documentation, physical or digital. This restricted the potential suspects in cases of IP theft, and it was usually an action targeted to specific documents or technology. The digitalization of IP information transfer and storage has opened the field to IP thieves in any location, allowing for either targeted or opportunistic attacks [6], and allowing attackers to operate in relative anonymity. The pool of suspects is thus far greater, and can include competitors, hackers that do this for money or fun, or even nation-states.

Resilience frameworks have addressed the way a supply chain responds over time to disruption events. Sheffi and Rice [7] described the extent of the consequences derived from a supply chain disruption as derived from the depth and duration of a negative evolution of performance resulting from the disruption, in what they named the "disruption curve". This curve implied that an improved response to disruption would consist of both a shorter and a shallower disruption in performance.

Despite being only qualitative, this approach contrasts to other supply chain resilience frameworks that identify resources and strategies, but do not address the measurement of the evolution of performance [8][9][10].

These resilience frameworks appear to be ill-suited for the challenges presented by cyber-risks in complex supply networks: by focusing on the expected resulting states and pre-existing resources required for a resilient response, the capabilities required to activate, drive and control the response have been comparatively overlooked.

Additionally, the case study method, despite being a very valuable tool for inductively extracting non-structured data about the response to disruptions, lacks a focus on the evolution of this response over time.

Literature has therefore mentioned the potential for complementarity of the case study method with other methods, such as system dynamics [11].

Derived from these gaps, this paper contributes by analyzing a specific case of IP theft resulting from a cyber-attack and looking into some of the concrete organizational structures that drive the resilient response of the organization to this theft. This process results in a dynamic model, and a categorization and sensibility analysis of this structure on the resulting performance

evolution over time. Second, in the process of building this dynamic model starting from the case study description of the IP theft, this paper aims to outline a structured method for "translating" case studies into dynamic response structures that can be quantified and modeled.

The structure of this paper is as follows: section II will describe the methodology; section III will describe the results; section IV will discuss and highlight implications of the results, and describe the limitations of the method, and section V will outline the conclusions and areas of future work.

II. METHODOLOGY

This paper uses the system dynamics (SD) framework to develop a dynamic model representation of a case study. This complementarity is particularly well suited for cases where there is little or no historic information, and where the evolution of performance is a relevant subject of study.

SD is a framework for the representation of systems that change over time by using a network of variables in relationships of circular causality; network composed of fundamentally two types of variables, stocks (accumulations) and flows either flowing into or out of these accumulations. By virtue of different timescales or the specific problem under question, it is sometimes convenient to represent some of these stocks or flows either as constants, or auxiliary variables (instantaneously changing).

The visible state for such a system is therefore completely represented by the values of the stocks in the system and all changes in these stocks is what can be understood as the system's "behavior". These conditions have two very relevant consequences: 1) By virtue of this networked representation, all the behaviors of a system are the direct result of its own structure, in what is termed the "endogenous" view of behavior in SD and 2) any system that changes over time in any interesting way, has at least one feedback loop (the basic circular causality unit) in its structure.

Despite being Forrester [12] who started what can be called the "MIT school" of thought in SD modeling, this paper will use the method outlined by [13], and proposes the following steps: problem articulation, formulation of a dynamic hypothesis, formulation of a dynamic model, testing, and policy design and evaluation.

The problem description and boundaries are obtained from documentation and interviews about the specific case study, and the data that can be extracted from these documents is "translated" into a causal loop diagram and a system dynamics model that is eventually simulated.

III. RESULTS

A. Case description

ABC Industries is a producer of hardware with 60.000 employees and a 12.2 percent operating margin. Six months before a product launch a federal agency informed ABC of a cyber-breach. The effect of this breach was the loss of IP data for 15 out of the 30 product lines. These lines were expected to contribute 25 percent of the company's total revenue for the next 5 years.

The stolen information allowed a hacker to exploit previously undiscovered design flaws, implant malicious code into these product lines, allow competitors to market a similar product earlier undercutting ABC on price.

ABC's reaction had three phases: Incident triage, Impact management and business recovery.

During the incident triage phase ABC brought in the necessary resources to assess the initial damage and prepare the organization for potential consequences of this attack. First, a team of managers and research scientists was formed to oversee the efforts to minimize the effects of this attack. This had negative effect on productivity. Second, an external cyber-security company was hired to investigate the leak, and patch the system to future similar attacks. Third, a law firm was hired to lay out the potential legal ramifications of the breach. Fourth, a public relations (PR) firm was hired to start preparing the commercial ramifications of this breach.

During the impact management phase ABC Industries changed the use of existing resources and processes. Product launch was accelerated by two months, creating a need for additional research personnel and overstretching the capacities of existing research personnel, decreasing productivity. Also, product shipments were suspended while an upgrade was developed for the products as a result of the stolen IP. Important contracts were lost probably as a result of both a decreased perception of product safety in the customers, and by the delayed shipment of existing orders. Contract losses were expected to account for 5 -10% of the projected revenues for the company.

During the recovery phase, ABC industries made structural changes as a result of the cyber-attack. First, it performed an inventory of all its IP, instituted an IP protection program, and upgraded its security infrastructure. Fig.1 shows an evolution of these actions.

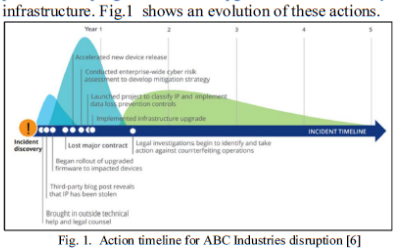

Fig. 1. Action timeline for ABC Industries disruption [6]

As a result of the cyber-attack, ABC industries reported additional costs of US$ 3.2 billion over 5 years. Despite their sales level returning to normal levels after

one year, the total recovery time was of five years. The following figure shows the evolution of the Sales and Profit levels with respect to the expected sales and profit levels, and is in essence the reference mode a dynamic model would seek to reproduce and explain.

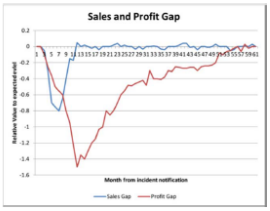

Fig. 2. Evolution of relative sales and profit levels during disruption

B. Model Development

From the case description, a series of circular causality feedback loop "types" can be identified (See Fig.3).

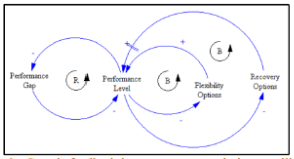

Fig. 3. Generic feedback loop types present during a resilient response

A first type corresponds to those feedback loops that form vicious circles with respect to the declining performance levels. An example of this is the loss of contracts derived from the IP theft: the more contracts or sales are lost, creates an even lower sales level increasing the sales gap and the profit gap.

A second type of feedback loops, are the "flexibility options" that the company uses to manage resources in the short term. The case mentions mainly management and R&D personnel as the internal resources involved, and PR, cyber-security consultants and legal counsel as external resources. The type two feedback loops can be further subdivided into either 1) a redistribution of internal resources (as in the short term there has been limited time to increase these resources), or the hiring of external resources, available quickly, but at additional cost, such as the case of the public relations firm, the cyber-security company and the Law consultant. Both of these options have an effect on the performance, through a decrease in the IP generation productivity, and through the increase in operation costs, respectively.

A third type of feedback loops are those that the company uses to manage the long-term actions, which we have denominated the recovery options. Examples of this include the hiring of additional R&D personnel that was hired for the generation of additional IP. These have effects on costs and are the last ones to be maintained until the company reaches the expected operation level. Figure 3 shows a causal loop diagram (CLD) representing these generic feedback loop types.

The specific loops identified in the description are shown in Table 1.

Table. 1. Feedback loops identified in description

Loop Number	Loop Type	Loop Number	Loop Name
1	Reinforcing	R1	IP Rules
2	Reinforcing	R2	PR to the rescue
1	Balancing	B1	Marketing Stabilizer
2	Balancing	B2	IP Expiration
3	Balancing	B3	Marketing Costs
4	Balancing	B4	Hacker Attacks
5	Balancing	B5	Trust issues
6	Balancing	B6	Productivoty Loss
7	Balancing	B7	Security Costs
8	Balancing	B8	Legal Bundle
9	Balancing	B9	Legal cousel
10	Balancing	B10	Legal costs
11	Balancing	B11	PR Costs
12	Balancing	B12	Leak containment

These Feedback loops represent the circular causality structures present in the case description, connecting relevant variables as seen in Fig.4.

In order to start building a dynamic model derived a first approach considers only the basic loops that create the base behavior, as shown in Fig. 5. The interaction of these loops tells a story of how a resilient behavior comes about without a disruption.

R1, reinforcing loop 1, "IP Rules" feedback loop. This is the main mechanism through which a company based in exclusive IP develops its business. Exclusive IP generates a Demand which is translated into Actual Sales and Actual Profit levels, which are partially invested into the development of more Exclusive IP, expanding the business

R1, reinforcing loop 1, "IP Rules" feedback loop. This is the main mechanism through which a company based in exclusive IP develops its business. Exclusive IP generates a Demand which is translated into Actual Sales and Actual Profit levels, which are partially invested into the development of more Exclusive IP, expanding the business

B1, balancing loop 1, "Marketing stabilizer" feedback loop. This captures the main mechanism ABC Industries uses to counteract differences in demand. Since the development of IP is a long, uncertain process, which is then reflected as exclusive products to the market, the way in which demand fluctuations are counteracted are through changes in the sales strategy through the use of marketing instruments, creating a loop that does not let the Sales Gap to increase endlessly.

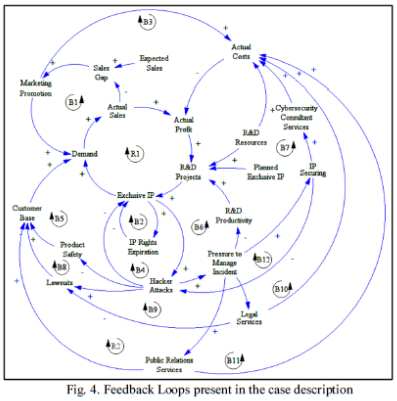

Fig. 4. Feedback Loops present in the case description

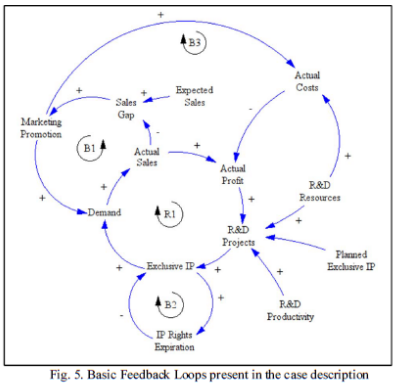

Fig. 5. Basic Feedback Loops present in the case description

B2, balancing loop 2, "IP expiration" feedback loop. This captures the process of IP expiration, resulting from the limited time for which an IP is exclusive to the company that created it.

B3, balancing loop 3, "Marketing Costs" feedback loop. This captures additional marketing costs, which limits the amount of marketing possible as it affects the profit level with a direct consequence in the number of R&D projects that can be started.

The resulting Dynamic model considering these base loops is shown in Fig. 6. The loops correspond to those in the CLD in Fig. 5.

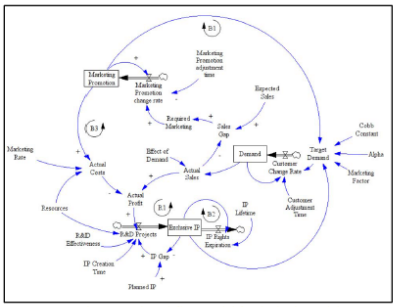

Fig. 6. Stock-and-flow model for the basic model

IV. DISCUSSION

A dynamic model can be validated in a variety of ways, as it has been documented by Senge and Forrester [14].

In this case, the base model was tested from equilibrium for an initial disruption in the level of Exclusive IP stock, and different levels of some of its exogenous variables, i.e., marketing feedback, customer adjustment time and marketing contract times. The resulting Sales Gap for this sensitivity analysis is shown in the following graphs.

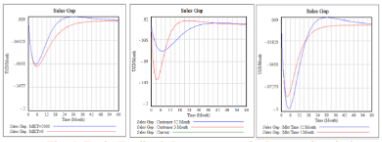

Fig. 4. Basic Feedback Loops present in the case description

Marketing contract time had extreme values of 1 and 12 months, customer adjustment time had variations from 3 to 12 months, and the Marketing Rate had a range of 0 to 2000.

The evolution over time of the sales gap resembles the behavior mode indicated during the case description in Fig. 2. Given the negative feedback loops present a slight over shoot is seen in all cases for one of the extreme values, and the sales gap recovers the desired level after close to 18 months

Despite only considering the feedback loops in Fig.5 from all the ones present in the case description, this basic model points the way forward for broadening and deepening the dynamic representation of the case study. The additional feedback loops should be introduced sequentially, testing how the model behavior is affected by each addition.

This process also illustrates a possible path from Case study to Dynamic Model, summarized as the iterative process of extracting the mental models present in the data, and creating maps of circular causality that drive processes over time: identify the actions from the case, identify the perceived causality of those actions and the variables that are affected in the process. Then by differentiating those variables that are slow to change from those that change quickly, the stock and flow diagram can be attempted.

The data gathering process for this paper revealed two interesting shortcomings with respect to the information available in a case study: 1) the descriptions imply causality without exploring it explicitly. It follows that the information contained in the way in which agents in the system assume the system works, is not gathered 2) There is an idealized process described as a unification of different data sources, obscuring a very important source of unexplained behavior in systems, this being the misalignment between mental models of agents acting in the same system. The contradictions should not be discarded, but rather compared and accounted for, as these might very probably have some influence in "unexplained" system behaviors.

V. CONCLUSION

By developing of a dynamic model based on a specific case study about the resilient response to a cyber-attack, this paper has shown the process of such an approach for representing cross-disciplinary processes that occur when an organization has to manage disruptions. Additionally it has put forward an initial approach for understanding the structure in an organization behind a resilient behavior.

Reaction design will involve the identification of these and other structures, obtaining adequate values for it governing exogenous variables; a crucial activity that will need to be internalized by organizations.

The suitability of undertaking a medium to long-term timeframe analysis of the problems related to the effects of cyber risks in operations, as well as the limited information available about past events of resilient response to cyber-attacks, make SD an attractive tool since it is a methodology less concerned with reproducing past behavior, focusing rather on the structures underlying the observed behavior, through the identification and explicit representation of the mental and formal models present in the organization.

The effect of considering a long-term view, beyond the immediate short term operational pressures, both allows for designing a response that minimizes the overall cost of a disruption, and identifies incentive structures that promote this response.

REFERENCES

[1] G. C. Stevens and M. Johnson, "Integrating the Supply Chain … 25 years on," International Journal of Physical Distribution & Logistics Management, vol. 46, no. 1, pp. 19–42, Aug. 2016.

[2] N. G. Leveson, Safeware: system safety and computers: Boston, Mass.: Addison-Wesley, 2001.

[3] "News Releases," Annual Study of Intangible Asset Market Value from Ocean Tomo, LLC. [Online]. Available: http://www.oceantomo.com/2015/03/04/2015-intangible-asset-market-value-study/. [Accessed: 31-May-2017].

[4] N. Kossovsky, B. Brandegee, and J. C. Giordan, "Using the market to determine IP's fair market value," Research-Technology Management, vol. 47, no. 3, pp. 33–42.

[5] "Net Losses: Estimating the Global Cost of Cybercrime," Global Initiative, 25-Jan-2017. [Online]. Available: http://globalinitiative.net/documents/net-losses-estimating-the-global-cost-of-cybercrime/. [Accessed: 01-Jun-2017].

[6] J. Gelinne, "The hidden costs of an IP breach: Cyber theft and the loss of intellectual property," DU Press. [Online]. Available: https://dupress.deloitte.com/dup-us-en/deloitte-review/issue-19/loss-of-intellectual-property-ip-breach.html. [Accessed: 01-Jun-2017].

[7] Y. Sheffi and J. B. Rice, "A Supply Chain View of the Resilient Enterprise," MIT Sloan Management Review. [Online]. Available: http://sloanreview.mit.edu/article/a-supply-chain-view-of-the-resilient-enterprise/. [Accessed: 01-Jun-2017].

[8] M. Christopher and H. Peck, "Building the Resilient Supply Chain," The International Journal of Logistics Management, vol. 15, no. 2, pp. 1–14, 2004.

[9] C. W. Craighead, J. Blackhurst, M. J. Rungtusanatham, and R. B. Handfield, "The Severity of Supply Chain Disruptions: Design Characteristics and Mitigation Capabilities," Decision Sciences, vol. 38, no. 1, pp. 131–156, 2007.

[10] J. Blackhurst, K. S. Dunn, and C. W. Craighead, "An Empirically Derived Framework of Global Supply Resiliency," Journal of Business Logistics, vol. 32, no. 4, pp. 374–391, 2011.

[11] G. Papachristos, "Case study and system dynamics research: Complementarities, pluralism and evolutionary theory development," 30th International Conference of the System Dynamics Society., vol. 112, 2012.

[12] J. W. Forrester, Industrial dynamics. Cambridge, MA: Pegasus, 1961.

[13] J. D. Sterman, Business dynamics: systems thinking and modeling for a complex world. Boston: McGraw-Hill/Irwin, 2000.

[14] J. W. Forrester and P. M. Senge, Tests for building confidence in system dynamics models. Cambridge, MA: System Dynamics Group, Sloan School of Management, Massachusetts Institute of Technology, 1978.

11.7 Complete list of articles in the synthesis sample

Year	Journal	Type (J/C/B)	Citation (Harvard)
2000	International Journal of Physical Distribution & Logistics Management	Journal Article	Warren, M. and Hutchinson, W., 2000. Cyber-attacks against supply chain management systems: a short note. International Journal of Physical Distribution & Logistics Management, 30(7/8), pp.710-716.
2002	International Journal of Physical Distribution & Logistics Management	Journal Article	Williams, L.R., Esper, T.L. and Ozment, J., 2002. The electronic supply chain: Its impact on the current and future structure of strategic alliances, partnerships and logistics leadership. International Journal of Physical Distribution & Logistics Management, 32(8), pp.703-719.
2006	Risk analysis	Journal Article	Andrijcic, E. and Horowitz, B., 2006. A Macro-Economic Framework for Evaluation of Cyber-security Risks Related to Protection of Intellectual Property. Risk analysis, 26(4), pp.907-923.

Year	Journal	Type (J/C/B)	Citation (Harvard)
2006	Quality of Protection	Journal Article	McQueen, M.A., Boyer, W.F., Flynn, M.A. and Beitel, G.A., 2006. Time-to-compromise model for cyber-risk reduction estimation. In Quality of Protection (pp. 49-64). Springer, Boston, MA.
2010	Report	Journal Article	Goldman, H.G., 2010. Building secure, resilient architectures for cyber mission assurance. *The MITRE Corporation*.
2011	In Internet of things (iThings/CPSCom)	Conference Article	Zhu, B., Joseph, A. and Sastry, S., 2011, October. A taxonomy of cyber attacks on SCADA systems. In Internet of things (iThings/CPSCom), 2011 international conference on and 4th international conference on cyber, physical and social computing (pp. 380-388). IEEE.
2011	In Technologies for Homeland Security (HST)	Conference Article	Goldman, H., McQuaid, R. and Picciotto, J., 2011, November. Cyber-resilience for mission assurance. In Technologies for Homeland Security (HST), 2011

Year	Journal	Type (J/C/B)	Citation (Harvard)
			IEEE International Conference on (pp. 236-241). IEEE
2011	In Decision and Control and European Control Conference (CDC-ECC)	Conference Article	Zhu, Q. and Başar, T., 2011, December. Robust and resilient control design for cyber-physical systems with an application to power systems. In Decision and Control and European Control Conference (CDC-ECC), 2011 50th IEEE Conference on (pp. 4066-4071). IEEE.
2012	Network Security	Journal Article	de Crespigny, M., 2012. Building cyber-resilience to tackle threats. Network Security, 2012(4), pp.5-8.
2012	In Intelligence and Security Informatics Conference (EISIC)	Conference Article	Rajamäki, J., Rathod, P., Ahlgren, A., Aho, J., Takari, M. and Ahlgren, S., 2012, August. Resilience of cyber-physical system: A case study of safe school environment. In Intelligence and Security Informatics Conference (EISIC), 2012 European (pp. 285-285). IEEE.

Year	Journal	Type (J/C/B)	Citation (Harvard)
2013	Environment Systems and Decisions	Journal Article	Kelic, A., Collier, Z.A., Brown, C., Beyeler, W.E., Outkin, A.V., Vargas, V.N., Ehlen, M.A., Judson, C., Zaidi, A., Leung, B. and Linkov, I., 2013. Decision framework for evaluating the macroeconomic risks and policy impacts of cyber attacks. Environment Systems and Decisions, 33(4), pp.544-560.
2013	Environment Systems and Decisions	Journal Article	Collier, Z.A., Linkov, I. and Lambert, J.H., 2013. Four domains of cybersecurity: a risk-based systems approach to cyber decisions. Environment Systems and Decisions, 4(33), pp.469-470.
2013	Environment Systems and Decisions	Journal Article	Linkov, I., Eisenberg, D.A., Plourde, K., Seager, T.P., Allen, J. and Kott, A., 2013. Resilience metrics for cyber systems. Environment Systems and Decisions, 33(4), pp.471-476.

Year	Journal	Type (J/C/B)	Citation (Harvard)
2013	In Nordic Conference on Secure IT Systems	Conference Article	Krotofil, M. and Cárdenas, A.A., 2013, October. Resilience of process control systems to cyber-physical attacks. In Nordic Conference on Secure IT Systems (pp. 166-182). Springer, Berlin, Heidelberg.
2013	Information & Security	Journal Article	Urciuoli, L., Männistö, T., Hintsa, J. and Khan, T., 2013. Supply Chain Cyber-security-Potential Threats. Information & Security, 29(1), p.51.
2013	Politics	Journal Article	Herrington, L. and Aldrich, R., 2013. The future of cyber-resilience in an age of global complexity. Politics, 33(4), pp.299-310.
2013	In Technologies for Homeland Security (HST)	Conference Article	Ramuhalli, P., Halappanavar, M., Coble, J. and Dixit, M., 2013, November. Towards a theory of autonomous reconstitution of compromised cyber-systems. In Technologies for Homeland Security (HST), 2013 IEEE

Year	Journal	Type (J/C/B)	Citation (Harvard)
			International Conference on (pp. 577-583). IEEE.
2013	Environment Systems and Decisions	Journal Article	Pawlak, P. and Wendling, C., 2013. Trends in cyberspace: can governments keep up?. Environment Systems and Decisions, 33(4), pp.536-543.
2014	The Electricity Journal	Journal Article	Onyeji, I., Bazilian, M. and Bronk, C., 2014. Cyber-security and critical energy infrastructure. The Electricity Journal, 27(2), pp.52-60.
2014	Journal of business continuity & emergency planning	Journal Article	Mallinder, J. and Drabwell, P., 2014. Cyber security: A critical examination of information sharing versus data sensitivity issues for organisations at risk of cyber attack. Journal of business continuity & emergency planning, 7(2), pp.103-111.

Year	Journal	Type (J/C/B)	Citation (Harvard)
2014	Technovation	Journal Article	Boyson, S., 2014. Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. Technovation, 34(7), pp.342-353.
2014	Computer	Journal Article	Collier, Z.A., DiMase, D., Walters, S., Tehranipoor, M.M., Lambert, J.H. and Linkov, I., 2014. Cybersecurity standards: managing risk and creating resilience. Computer, 47(9), pp.70-76.
2014	Journal of business continuity & emergency planning	Journal Article	Hult, F. and Sivanesan, G., 2014. Introducing cyber. Journal of business continuity & emergency planning, 7(2), pp.97-102.
2014	In Resilient Control Systems (ISRCS)	Conference Article	Fink, G.A., Griswold, R.L. and Beech, Z.W., 2014, August. Quantifying cyber-resilience against resource-exhaustion attacks. In Resilient Control Systems (ISRCS), 2014 7th International Symposium on (pp. 1-8). IEEE.

Year	Journal	Type (J/C/B)	Citation (Harvard)
2014	International Journal of Research in Engineering and Applied Sciences	Journal Article	Aggarwal, P., Arora, P. and Ghai, R., 2014. Review on cyber crime and security. International Journal of Research in Engineering and Applied Sciences, 2(1), pp.48-51.
2014	Technovation	Journal Article	Rongping, M. and Yonggang, F., 2014. Security in the cyber supply chain: A Chinese perspective. Technovation, 7(34), pp.385-386.
2014	Technovation	Journal Article	Williams, C., 2014. Security in the cyber supply chain: Is it achievable in a complex, interconnected world?. Technovation, 34(7), pp.382-384.
2014	Technovation	Journal Article	Venter, H.S., 2014. Security issues in the security cyber supply chain in South Africa. Technovation, 7(34), pp.392-393.
2014	Journal of business continuity & emergency planning	Journal Article	Hult, F. and Sivanesan, G., 2014. What good cyber-resilience looks like. Journal of business continuity & emergency planning, 7(2), pp.112-125.

Year	Journal	Type (J/C/B)	Citation (Harvard)
2015	International Journal of Computer Networks & Communications	Journal Article	Abraham, S. and Nair, S., 2015. A PREDICTIVE FRAMEWORK FOR CYBER SECURITY ANALYTICS USING ATTACK GRAPHS. International Journal of Computer Networks & Communications, 7(1), p.1.
2015	In Proceedings of the 2015 Workshop on Automated Decision Making for Active Cyber Defense	Conference Article	Choudhury, S., Rodriguez, L., Curtis, D., Oler, K., Nordquist, P., Chen, P.Y. and Ray, I., 2015, October. Action recommendation for cyber-resilience. In Proceedings of the 2015 Workshop on Automated Decision Making for Active Cyber Defense (pp. 3-8). ACM.
2015	International Journal of Computer, Electrical, Automation, Control and Information Engineering	Journal Article	Ahmad, A., Johnson, C. and Storer, T., 2015. An Investigation on Organisation Cyber-resilience. World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering, 9(7), pp.1703-1708.

Year	Journal	Type (J/C/B)	Citation (Harvard)
2015	Technology Innovation Management Review	Journal Article	Davis, A., 2015. Building cyber-resilience into supply chains. Technology Innovation Management Review, 5(4), p.19.
2015	Journal of business continuity & emergency planning	Journal Article	Ferdinand, J., 2015. Building organisational cyber-resilience: A strategic knowledge-based view of cyber security management. Journal of business continuity & emergency planning, 9(2), pp.185-195.
2015	Technology Innovation Management Review	Journal Article	Jensen, L., 2015. Challenges in Maritime Cyber-Resilience. Technology Innovation Management Review, 5(4), p.35.
2015	In Proceedings of the 2015 Workshop on Automated Decision Making for Active Cyber Defense	Conference Article	Khan, Y.I., Al-Shaer, E. and Rauf, U., 2015, October. Cyber-resilience-by-Construction: Modelling, Measuring & Verifying. In Proceedings of the 2015 Workshop on Automated Decision Making for Active Cyber Defense (pp. 9-14). ACM.

Year	Journal	Type (J/C/B)	Citation (Harvard)
2015	Technology Innovation Management Review	Journal Article	Urciuoli, L., 2015. Cyber-resilience: a strategic approach for supply chain management. Technology Innovation Management Review, 5(4), p.13.
2015	Technology Innovation Management Review	Journal Article	Boyes, H., 2015. Cybersecurity and cyber-resilient supply chains. Technology Innovation Management Review, 5(4), p.28.
2015	Technology Innovation Management Review	Journal Article	Khan, O. and Estay, D.A.S., 2015. Supply chain cyber-resilience: Creating an agenda for future research. Technology Innovation Management Review, 5(4).
2015	Environment Systems and Decisions	Journal Article	DiMase, D., Collier, Z.A., Heffner, K. and Linkov, I., 2015. Systems engineering framework for cyber physical security and resilience. Environment Systems and Decisions, 35(2), pp.291-300.
2016	Journal of business continuity & emergency planning	Journal Article	Brown, H.S., 2016. After the data breach: Managing the crisis and mitigating the impact. Journal of

Year	Journal	Type (J/C/B)	Citation (Harvard)
			business continuity & emergency planning, 9(4), pp.317-328.
2016	Journal of Cyber Policy	Journal Article	Tiirmaa-Klaar, H., 2016. Building national cyber-resilience and protecting critical information infrastructure. Journal of Cyber Policy, 1(1), pp.94-106.
2016	Computers & Security	Journal Article	Tran, H., Campos-Nanez, E., Fomin, P. and Wasek, J., 2016. Cyber-resilience recovery model to combat zero-day malware attacks. *computers & security*, *61*, pp.19-31.
2016	Business Information Review	Journal Article	Wilding, N., 2016. Cyber-resilience: How important is your reputation? How effective are your people?. Business Information Review, 33(2), pp.94-99.
2016	Proceedings of the IEEE	Journal Article	Harrison, R., Vera, D. and Ahmad, B., 2016. Engineering methods and tools for cyber–physical automation systems. Proceedings of the IEEE, 104(5), pp.973-985.

Year	Journal	Type (J/C/B)	Citation (Harvard)
2016	Renewable and Sustainable Energy Reviews	Journal Article	Arghandeh, R., von Meier, A., Mehrmanesh, L. and Mili, L., 2016. On the definition of cyber-physical resilience in power systems. Renewable and Sustainable Energy Reviews, 58, pp.1060-1069.
2016	In Systems and Information Engineering Design Symposium (SIEDS)	Conference Article	Barron, S., Cho, Y.M., Hua, A., Norcross, W., Voigt, J. and Haimes, Y., 2016, April. Systems-based cyber security in the supply chain. In Systems and Information Engineering Design Symposium (SIEDS), 2016 IEEE (pp. 20-25). IEEE.
2016	In Dependable Systems and Networks Workshop	Conference Article	Avizienis, A., Avizienis, R. and Avizienis, A.V., 2016, June. The Concept of a Software-Free Resilience Infrastructure for Cyber-Physical Systems. In Dependable Systems and Networks Workshop, 2016 46th Annual IEEE/IFIP International Conference on (pp. 230-233). IEEE.

Year	Journal	Type (J/C/B)	Citation (Harvard)
2017	Pervasive and Mobile Computing	Journal Article	Wang, J., Hui, L.C., Yiu, S.M., Wang, E.K. and Fang, J., 2017. A survey on cyber attacks against nonlinear state estimation in power systems of ubiquitous cities. Pervasive and Mobile Computing, (39), pp.52-64.
2017	Supply Chain Management: An International Journal	Journal Article	Ali, A., Ali, A., Mahfouz, A., Mahfouz, A., Arisha, A. and Arisha, A., 2017. Analysing supply chain resilience: integrating the constructs in a concept mapping framework via a systematic literature review. Supply Chain Management: An International Journal, 22(1), pp.16-39.
2017	Journal of Water Resources Planning and Management	Journal Article	Taormina, R., Galelli, S., Tippenhauer, N.O., Salomons, E. and Ostfeld, A., 2017. Characterizing Cyber-Physical Attacks on Water Distribution Systems. Journal of Water Resources Planning and Management, 143(5), p.04017009.

Year	Journal	Type (J/C/B)	Citation (Harvard)
2017	Production Engineering	Journal Article	Lee, J., Jin, C. and Bagheri, B., 2017. Cyber physical systems for predictive production systems. Production Engineering, 11(2), pp.155-165.
2017	International Journal of Critical Infrastructure Protection	Journal Article	Peter, A.S., 2017. Cyber-resilience preparedness of Africa's top-12 emerging economies. International Journal of Critical Infrastructure Protection, 17, pp.49-59.
2017	In ICMLG2017 5th International Conference on Management Leadership and Governance	Conference Article	Conklin, W.A., Shoemaker, D. and Kohnke, A., 2017. Cyber-resilience: Rethinking Cybersecurity Strategy to Build a Cyber Resilient Architecture. In ICMLG2017 5th International Conference on Management Leadership and Governance (p. 105). Academic Conferences and publishing limited.
2017	Computer Science Review	Journal Article	Marotta, A., Martinelli, F., Nanni, S., Orlando, A. and Yautsiukhin, A., 2017. Cyber-insurance survey. Computer Science Review.

Year	Journal	Type (J/C/B)	Citation (Harvard)
2017	Proceedings of the IEEE	Journal Article	Ashok, A., Govindarasu, M. and Wang, J., 2017. Cyber-Physical Attack-Resilient Wide-Area Monitoring, Protection, and Control for the Power Grid. Proceedings of the IEEE.
2017	Proceedings of the IEEE	Journal Article	Li, Z., Shahidehpour, M. and Aminifar, F., 2017. Cybersecurity in Distributed Power Systems. Proceedings of the IEEE.
2017	International Journal of Critical Infrastructure Protection	Journal Article	Chaves, A., Rice, M., Dunlap, S. and Pecarina, J., 2017. Improving the cyber-resilience of industrial control systems. International Journal of Critical Infrastructure Protection, 17, pp.30-48.
2017	Computers & Security	Journal Article	Ruan, K., 2017. Introducing cybernomics: A unifying economic framework for measuring cyber-risk. Computers & Security, 65, pp.77-89.
2017	Electronics	Journal Article	AlMajali, A., Viswanathan, A. and Neuman, C., 2016. Resilience Evaluation of Demand Response as

Year	Journal	Type (J/C/B)	Citation (Harvard)
			Spinning Reserve under Cyber-Physical Threats. Electronics, 6(1), p.2.
2017	International Journal of Interactive Multimedia & Artificial Intelligence	Journal Article	Pan, Y., White, J., Schmidt, D.C., Elhabashy, A., Sturm, L., Camelio, J. and Williams, C., 2017. Taxonomies for Reasoning About Cyber-physical Attacks in IoT-based Manufacturing Systems. International Journal of Interactive Multimedia & Artificial Intelligence, 4(3).
2017	IEEE Transactions on Smart Grid	Journal Article	Jin, D., Li, Z., Hannon, C., Chen, C., Wang, J., Shahidehpour, M. and Lee, C.W., 2017. Towards a Cyber Resilient and Secure Microgrid Using Software-Defined Networking. IEEE Transactions on Smart Grid.

11.8 Python routine XML-Data

```
# Python routine written to read the xml Tree structure
# that comes out of a XSTAMPP file

import xml.etree.ElementTree as ET
import csv

tree = ET.parse("XSTAMPP-Data.hazx")
root = tree.getroot()

# open a file for writing
data = open('Data-Out.csv', 'w')

chosen_set=["number","title","description","id"]
chosen_tree = 'controlaction'
chosen_subset=["description","id","number","type"]
chosen_subtree= 'unsafecontrolaction'

# create the csv writer object
csvwriter = csv.writer(data)

#data_head = []

#count = 0

for attribute in root:
                dataline =[]
                for item in attribute.iter('controlaction'):
                                for subitem in item.iter('unsafecontrolactions'):
                                                for param_value in
subitem.iter('unsafecontrolaction'):
                                                                value
=param_value.text
                                                                datapoint = value
                                dataline.append(datapoint)
                csvwriter.writerow(dataline)
data.close()
```

11.9 Research Protocol: Systemic Risk Analysis

v.170330

DTU

PhD project – Managing Cyber risk in the global supply chain

Research Protocol for Semi-structured interview

I. Objectives

The objective of this research protocol is to describe and prescribe a reproducible data gathering and analysis process within the study "Information structures and their systemic risk" in the context of the PhD research project "Managing cyber risk in the global supply chain" from the Department of Management Engineering at the Technical University of Denmark DTU.

The purpose of the study is twofold: 1) to gain some insight into the supply chain information structures that result in physical movement in the supply chain, and 2) the relationship of this structure change to the risk profile in that supply chain. This study will identify components of this structure by using semi-structured interviews and questionnaires. The interviews and questionnaire completion will be either through an hour-long face-to-face meeting, or an electronic meeting (e.g., Skype). The risk profile will be determined by the use of the systemic risk analysis methodology STAMP (Leveson, 2011).

Characteristics of the information structure being researched include information flows, information storage, regulating loops, delays and associated risks. The data gathering will be done for three scenarios: regular operations and two specific emergency scenarios: for the case where a relevant supplier is suddenly not available for one week, and the case when there is a sudden loss of internal production capacity for one week. The subjects of this research will be people in specific roles within supply chains with specific characteristics.

The research questions guiding this research are:

1.- What are the information structures that generate and regulate physical movement of goods and services in a supply chain?

2.- How does this information structure vary when there is an unexpected disruptive event?

3.- What is the connection between the risk profile and the reaction to disruptions in a supply chain?

4.- How aware are members of an organization of existing regulating loops in their activity with each other and with their supply chain?

II. Background and Rationale

Supply Chain processes are the physical movement of goods and services interdependent between human operators and information technology, and It has been well documented that supply chain operations are based on the underlying structure of coordinating information flows in the organization (Forrester, 1961; Sahin et al., 2002).

Research Protocol page 1 of 5 PhD Project

Disruptions to these coordinating flows, such as the ones created by cyber-attacks, can result in operational disruptions for cases where the supply chain reaction is insufficient. There is limited understanding on the relationship between underlying information structures in the supply chain, the risk these pose to supply chain operations for the case of an information flow disruption, and the reaction these supply chains adopt when faced with these disruptions.

This study seeks to contribute to the scientific development of a framework, based on the premise that organizational structure is the source of its visible behavior, by contributing empirical data on the information structures that result in physical movement of goods and services, during normal operations and during times of disruption.

III. Procedures

A. Research Design

The research is a descriptive and correlational and meta-analytical case study of a supply chain.

- It is descriptive as the data that will be gathered will mostly be a categorical non-numerical detail of the components of the supply chain;
- it is correlational as the analysis will look for the relationship between different components of the described structure and the types of responses these supply chains have during disruptions, and data will be gathered from multiple roles in the supply chain to decrease the threat if internal validity, i.e., minimizing the systematic error (bias) in the data that is gathered;
- it is meta analytical as the study considers the gathering of data from, and the comparative analysis of, multiple companies so as to decrease the threat of external validity, i.e., the capacity of generalizing the results of this research to organizations that did not take part in the research.

1.- The processes that will be studied are:

1a.- Sourcing process at the buyer (Request for Quotation, Purchasing, Shipping, Reception, Payment)
1b.- Sourcing process at the supplier (Quotation, Transport, Delivery, Documentation, Payment)

2.- For each of these processes, data will be gathered. The data will be recorded by voice if interviewee agrees, or notes will be taken of answers.

3.- The interaction will be guided by the Detailed Study Procedure described in Section D of this document.

B. Sample

The data will be gathered from as many of the following roles as possible in the supply chain:

B1.- Supply Chain Manager
B2.- IT Manager
B3.- Principal Buyer

v.170330

B4.- Outbound Specialist
B5.- Warehouse Manager / Operator
B6.- Finance

C. Measurement / Instrumentation

This study will use two instruments for the recording and measurement of the data.

C1.- Semi structured interview
C2.- Questionnaire
C3.- Group Workshop

D. Detailed study procedure

D1. For the semi-structured interviews:

1. Interview ID, Date, time and location
2. Identify Interviewer and Interviewee
3. Present the notes to the Interviewee
4. Present the purpose of the research
   "We will map the information flow structures at your organization and one important supplier"
   The data we will gather is:
   a. Which people and roles are involved in the organization
   b. Which information is exchanged
   c. Which processes result from this information flow
   d. Which control structures and feedback loops exist
   e. What is the frequency of these information flows
   f. What is the control hierarchy at this company and an important supplier
   g. What mediums are used to transfer information
   h. What is the mental model/process model of the interviewee
5. Ask the required Open Questions
   a. To which department do you belong and to which department do you talk to?
   b. In which processes are you actively involved?
   c. With whom do you work/share information and in which respective processes?
   d. Any process you are involved in during an emergency state?
6. Thank interviewee for their time
7. Transcribe interview results to format shown in Section G of this document.

v.170330

DTU

E. Threats to Validity

The threat to internal validity is addressed by the data gathering from different roles in the supply chain in independent interviews, so as to decrease systematic errors, i.e., bias.

The threat to external validity is addressed by the data gathering from multiple supply chains and by a comparative analysis of the results of the different case studies, so as to contribute to the generalizability of the results from this study.

F. Data Analysis

The data that is gathered in this process will be used in two main processes:

- Dynamic information flow mapping
- Modified STPA Systemic risk analysis based on the STAMP framework

G. Output Document for Transcription

The Transcription document will have the following sections.

- Title: Interview protocol
- Subtitle: First Interview – Detail about the information flows in the organization
- Interview ID
- Date
- Time
- Location
- Interviewer
- Interviewee
- Notes to Interviewee
- Purpose of research
- Questions
- Response from Interviewee to the specific questions:
  - To which department do you belong and to which department do you talk to?
  - In which processes are you actively involved?
  - With whom do you work/share information and in which respective processes?
  - Does any of this change in an emergency state?
- Detailed Information exchange (Other Notes)
- Other comments

IV. Bibliography

Forrester, J., 1961. Industrial Dynamics, System Dynamics Series, Pegasus Communications.

Leveson, N., 2011. Engineering a safer world: Systems thinking applied to safety. MIT press.

Rowley, J., 2012. Conducting research interviews. Management Research Review, 35(3/4), pp.260-271.

v.170330

Sahin, F. and Robinson, E.P., 2002. Flow coordination and information sharing in supply chains: review, implications, and directions for future research. Decision sciences, 33(4), pp.505-536.